Computers & Security 134 (2023) 103470

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

When expectation fails and motivation prevails: the mediating role of awareness in bridging the expectancy-capability gap in mobile identity protection

Yasser Alhelaly [a,*], Gurpreet Dhillon [b,c], Tiago Oliveira [a]

[a] NOVA Information Management School, Universidade Nova de Lisboa, Campus de Campolide, Lisboa 1070-312, Portugal
[b] G. Brint Ryan College of Business, University of North Texas, Denton, TX 76203-5017, United States
[c] University of KwaZulu-Natal, Durban, South Africa

ARTICLE INFO

Keywords:
Information Security
Mobile Identity Protection
Expectancy-Value Theory
Protection Awareness
Protection Experience
Qualitative Research
Quantiative Research
Mixed Methods

ABSTRACT

Identity theft poses a significant threat to mobile users, yet mobile identity protection is often overlooked in cybersecurity literature. Despite various technical solutions proposed, little attention has been given to the motivational aspects of protection. Moreover, the disparity between individuals' expectations and their ability to safeguard their mobile identities exacerbates the problem. This study adopts a mixed-methods approach and draws on expectancy-value theory to address these gaps and explore the impact of expectations, capabilities, motivational values, technical measures, and awareness on individuals' intentions to achieve mobile identity protection. Our research reveals that protection awareness acts as a crucial mediator between individuals' expectations and capabilities. Additionally, motivational values not only enhance technical protection measures but also significantly influence identity protection intentions. Furthermore, we identify the moderating effect of protection experience on individuals' expectations and perceived value of identity protection. This study contributes to mobile security literature by highlighting the pivotal role of protection awareness in bridging the divide between individual expectations and actual capabilities in mobile identity protection.

1. Introduction

The proliferation of smartphones and their increasing role in our lives necessitates a comprehensive approach to address the problem of mobile theft and emphasizes the significance of mobile identity protection. According to the Ericsson Mobility Report, smartphone users worldwide are projected to reach 6.84 billion by 2023, with an expected annual growth rate of 4.2% (Ericson, 2023). This widespread adoption of smartphones has led governments to rely more on mobile identity in their services. According to Gartner, at least a third of national governments and half of U.S. states will offer citizens mobile-based identity wallets by 2024 (Gartner, 2022).

The growing dependence on smartphones makes them a prime target for hackers and cybercriminals. Malicious apps, phishing attempts, and social engineered identity theft attacks are just some of the methods used to target mobile devices and compromise personal information. Therefore, securing mobile phones and, more specifically, protecting mobile identity has become paramount. However, the lack of awareness among smartphone users regarding their data being collected puts them at a higher risk of falling victim to identity theft. The issue of mobile identity theft is widespread, with a Kaspersky Mobile Threats Report in 2020 revealing a significant increase in malicious installers, including mobile banking trojans (Kaspersky, 2020). Therefore, organizations need to invest in robust mobile identity protection measures to prevent data breaches and safeguard their customers' sensitive information.

Despite the increasing incidents of mobile identity theft, the extant literature has only recently started addressing this topic. Kraus et al. (2017) suggest that protective behavior depends on context and usage motives, and not only on secure devices and implemented security procedures. Similarly, Braver et al. (2014) suggest a cross-disciplinary approach using motivation-based theoretical concepts to study identity protection. This study suggests that there are two gaps in mobile identity protection. The first gap is the protection expectancy-capability gap. In this case, individuals believe they can protect themselves but may lack the necessary capabilities to do so. The second gap is the technical-motivation means protection. This gap refers to the imbalance

* Corresponding author.
E-mail address: yalhelaly@novaims.unl.pt (Y. Alhelaly).

https://doi.org/10.1016/j.cose.2023.103470
Received 8 May 2023; Received in revised form 21 July 2023; Accepted 3 September 2023
Available online 9 September 2023

between the predominant reliance on technical solutions for addressing identity theft while neglecting the crucial role of motivation in effectively mitigating the problem.

Therefore, this paper aims to address these gaps by examining the role of motivation and awareness in resolving mobile identity theft. Drawing on the expectancy-value theory of motivation (Vroom, 1964), this research advances the concept of mobile security and, more specifically, mobile identity protection by developing and examining the proposed gaps model using a mixed-methods approach. Ultimately, this research aims to provide insights into effective mobile identity protection strategies for organizations emphasizing the significant role of awareness in bridging the gaps between individuals' expectations and their protection capabilities. It also considers using both the technical and motivational aspects of mobile identity protection to mitigate theft attacks and cybersecurity risks.

The contribution of the work can be summarized as follows:

- Individual protection awareness bridges the gap between individual expectations and actual capabilities for protecting their mobile identity by mediating the relationship between expectancy-capability and technical-motivation protections on one side and individual intentions for mobile identity protection on the other.
- The motivational aspects of identity protection values greatly influence a person's intentions toward mobile identity protection. Furthermore, accomplishment and intrinsic and extrinsic motivations are the determinants of the motivational aspects of mobile identity protection values.
- Individual experiences with mobile identity protection have a negative moderating effect on the relationship between expectancy and motivational intentions for identity protection. However, the relationship between perceived value and identity protection motivation intentions has a positive moderation effect.

2. Background and Theoretical Framing

Two bodies of literature inform our work. The first is the burgeoning literature on online identity and its extensions. The second is the role of Expectancy-Value Theory (EVT) literature and its role in mobile identity protection posture. In the paragraphs below, we discuss each of the two bodies of literature focusing on (1) mobile identity context and related threats, (2) mobile identity protection literature gaps, and 3) mobile identity protection behavior. Finally, we position our argument given the debates in the extant literature. Fig. 1 shows the framing of the study, starting with a review of existing literature to identify mobile identity protection gaps and associated sources. In-depth interviews are then conducted to explore relevant concepts and develop hypotheses. Finally, a survey is utilized to examine the developed model and validate the findings, completing the research framework.

2.1. The importance of mobile identity context

With more than 7.26 billion unique mobile subscribers worldwide in 2022[1], mobile devices are becoming the future of digital identity. Mobile identity is an extension of the concept of digital identity that illuminates the importance of mobility (Roussos et al., 2003). Mobile identity is defined as the application of a user's identity attributes bound to a mobile device for identity verification, authentication, and/or authorization that enables an end-user to access information and resources while using different mobile devices. Feher (2019) discusses mobile identity as a reference for digital identity. He argues that mobile identity has two important aspects, smart identity technologies (e.g., smartphones) and data-driven services. Also, Carter and Grover (2015) refer to digital identity as mobile phone identity, which is identified as a product of how mobile users interact with their phones, and a force affecting the way individuals interact with the world around them.

Mobile identity enables access to more online services, ensures financial inclusion, and allows individuals to transact at any time and from any location. A mobile identity consists of two primary components: (1) User information as biometric characteristics, digitized government identity credentials, or financial account data, and (2) Mobile device information as geolocation, mobile or device ID number.

The importance of mobile identity protection against theft attacks has increased in the last few years due to the vast increase in data breaches. In a recent study, Bubukayr and Almaiah (2021) suggest that protection on smartphones is important due to the amount of significant data they hold. They suggest that the number of people using smartphones and apps is gradually increasing and that this is due to the ease with which they may be used. They noted that users are increasingly performing sensitive and critical financial operations, making them a tempting target for hackers.

2.2. Mobile Identity Threats & Consequences

The widespread use of mobile devices in our daily lives has now extended to work settings, where concerns about security risks have become a growing issue. One such risk is identity theft, which is a concern for both individuals and organizations. According to researchers such as Bélanger and Crossler (2019), the increasing use of personal mobile devices in work settings has resulted in a rise in cyberattacks and data breaches that exploit mobile devices to gain unauthorized access to organizational networks. The mobile context presents unique challenges, with security risks posing significant threats that are greater than those in other contexts (Zhang et al., 2013). Security mechanisms available on mobile devices are also not yet fully mature (Virvilis et al., 2014), exposing mobile users to increased risks in their online activities. Recent studies by Ogbanufe and Pavur (2022) emphasize the criticality of mobile identity theft, as it can have far-reaching consequences on individuals' financial status. These consequences include the potential for attackers to use stolen mobile identities and sensitive data to commit cybercrimes and infect mobile devices with malicious tools to gain remote control (Leavitt, 2011). Given the difficulty in linking data breaches and identity theft attacks, identity theft is considered one of the most challenging threat to mobile users.

To perpetrate mobile identity theft, hackers may use a range of tools and techniques such as malware, phishing, SMS, emails, and spyware (Leavitt, 2011), as well as the more recent SIM swapping attack used to target the mobile identity of cryptocurrency holders (ENISA, 2020). In response to these threats, researchers have analyzed the features of identity theft and developed several innovative technical protective measures (Bose and Leung, 2019). For instance, the European Data Protection Board (EDPB) has recently launched a data protection guide for small businesses[2] that highlights the importance of implementing technical measures to protect the confidentiality of individuals' personally identifiable information against unauthorized access and use of data and breaches of confidentiality such as identity theft. In their guidelines, the EDPB suggested several technical protection measures, such as data anonymization, in which personal data can be rendered anonymous in such a manner that the individual is not or no longer identifiable. Data anonymization is a process that consists of using a set of techniques to make personal data anonymous in such a way that it becomes almost impossible to identify the person by any means that are reasonably likely to be used. In the same vein, Caruccio, et al. (2022) suggest that data anonymization could achieve the balance between data utilization and protection requirements. By applying

[1] https://www.statista.com/statistics/218984/number-of-global-mobile-users-since-2010/

[2] Secure personal data | European Data Protection Board (europa.eu)

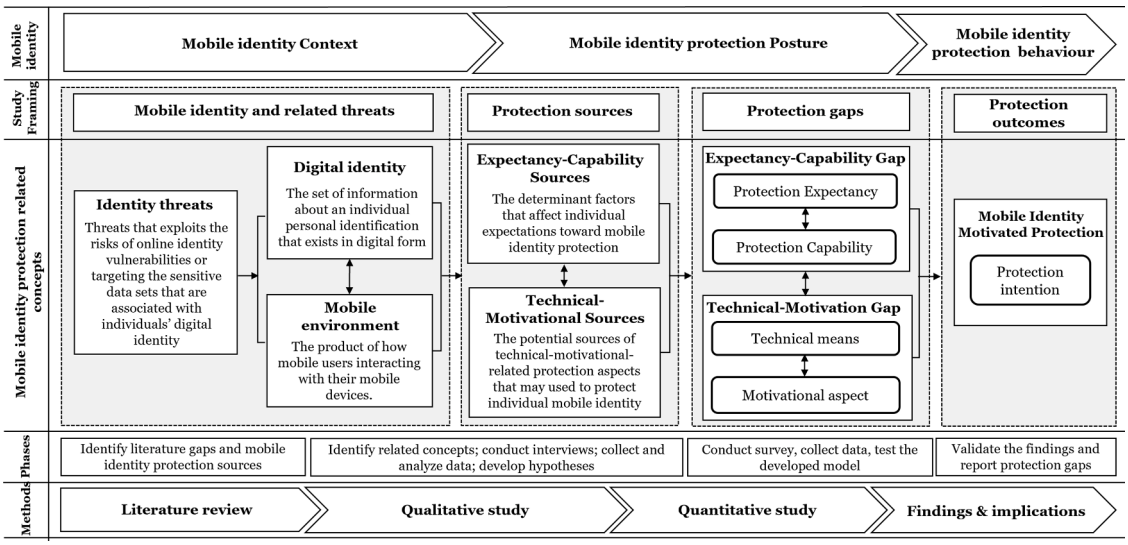

Fig. 1. The conceptual flow of the research.

anonymization techniques such as generalization, which involves aggregating or categorizing data, the specificity of personally identifiable information can be reduced, making it more challenging for attackers to associate sensitive data with individual identities when deploying identity theft attacks. Although many technical solutions have been proposed on the organizational level, few existing studies have examined the role of behavioral and motivational aspects in mobile identity protection on the individual level.

2.3. Mobile Identity Protection

Despite the growing attention given to protective behavior in the mobile context, there remains a significant gap between the conceptual and practical perspectives of mobile identity protection. Appendix 1 illustrates this gap by identifying two critical areas of concern: the conceptual gap, which relates to the expectancy-capability of individuals, and the practical gap, which pertains to the technical-motivation of individuals. To better understand these gaps, we will first discuss the Expectancy-Value Theory of motivation in the Information Systems literature before addressing the mobile identity protection gaps.

Information protection is the ability of an individual to safeguard their information assets from various threats. This study focuses on mobile identity as the most critical asset for mobile information security and examines how individuals' motivation to protect their mobile identities is influenced by their perceived expectations and values. According to Vroom's (1964) Expectancy-Value Theory, the strength of an individual's tendency to act in a particular way is determined by two factors: the expectancy of achieving a desired outcome through the behavior and the attractiveness or value of the outcome to the individual (Fox, 2007).

2.3.1. The expectancy-value theory of motivation

Several empirical studies have applied expectancy theory to study computer usage and decision support systems (e.g., Burton et al., 1992; Howard and Mendelow, 1991; Snead and Harrell, 1994). Melone's (1990) work suggests that EVT has the advantage of presenting a theoretical framework for examining user evaluative attitudes and their behavioral intention responses. This does not suggest that expectancy theory is the only applicable motivation theory. However, EVT theoretically resonates with our mobile identity protection context by conceptualizing the mobile users' intention toward identity protection. Appendix 2 summarizes the conceptualization of EVT in the Information Systems literature. In the next section, we use the motivational components of EVT as our theoretical framework to better understand an individual's protective behavior in the mobile context focusing on the protection gaps and related sources.

2.3.2. The expectancy-capability gap

Some scholars have noted a gap between an individual's expectations and reality (Nolan and Wetherbe, 1980; Trauth et al., 1993). They defined this gap as the "expectancy gap." Jiang et al. (2002) suggest that the expectancy gaps are expected to impact capabilities perceptions. Some seminal works in Information Systems have noted that there is an "expectation gap" between what individuals are expecting to accomplish and what they are capable of doing. For instance, Nolan and Wetherbe (1980) use the term *expectation gap* to highlight the considerable disadvantage in terms of managing expectations and technological reality in managing information systems. Trauth et al. (1993) also use the same term to confirm the existing gap between the skills required of future IS professionals and the actual graduates' abilities. The researchers attributed this expectation gap to problems with the relevance of Information Systems.

Serrano and Karahanna (2016) suggest that various terms appear in the literature to portray attributes of users and technology, such as characteristics, efficacy, abilities, and capabilities. In this research, the authors propose the term "protection capability" to capture the efficacy of mobile users in protecting their mobile identities. Jiang et al. (2002) suggest that expectation gaps are expected to impact capabilities perceptions. Hence, examining the expectancy capability gap is important to understand individuals' intentions toward mobile identity protection.

In psychology, individuals' expectancy to protect their mobile identity reflects their prejudgment that performing certain identity protection actions (e.g., enabling fingerprint lock on the smartphone) will protect a person's mobile identity (Bandura, 1997). While individuals' capabilities reflect their convictions about their ability to execute the identity protection measurement to secure their mobiles against different identity threats (Bandura, 1986), Bandura (1997) suggests that individual behaviors can be better predicted by the beliefs that they hold about their capabilities than by what they are capable of accomplishing. In his work, Bandura distinguishes between (1) the individual motivation to perform a target behavior based on expected outcomes of the behavior and (2) their perceived capability to perform the behavior.

Based on the above discussion, it is suggested that there is a gap between what individuals expect and the reality of what they can do. This gap is referred to as the *Expectancy-Capability Gap*. This gap can be a

significant source of frustration when it concerns individual identity protection in the mobile context. While many individuals may recognize the expectancy-capability gap, the existing literature overlooks this problem.

2.3.2.1. The expectancy-capability sources. As suggested previously, the discrepancy between individuals' expectations and actual capabilities creates the expectancy-capability gap. To examine this gap, the extant literature has been reviewed to identify the potential sources that predict individuals' capabilities to protect their mobile identity and the determinant factors that affect individual expectations toward identity protection in the mobile environment.

Landry (2003) suggests that individual expectations for a specific behavior reflect their belief about the consequences of that behavior. Feather (1982) theorized his motivational behavior model that emphasized an individual's expectancies. In his work, he suggests that the expectations of individuals for the outcomes may result from successfully performing the target behavior. Feather indicates that several factors influence the user's expectations to succeed in achieving mobile identity protection, such as 1) individuals' previous experiences, 2) the importance of the task, and 3) their self-confidence, predict their expectancy to succeed in the task.

2.3.3. The technical-motivation gap

In the mobile identity context, many technical-related protection solutions are proposed to counter the risks and vulnerabilities associated with mobile identity threats. These solutions are categorized on different levels ranging from technical-related solutions (e.g., operating systems security, identity management software, and advanced authentication) to motivational protective behavior of the mobile users (i.e., use of motivation concepts to influence protection behavior). In this study, the two categories of mobile identity protection refer to the technical means of protection and the motivational aspects of protection to identify the gaps between these two means.

2.3.3.1. The technical means of protection. The potent role of IT and, more specifically, smartphones and mobile devices in different aspects of our daily lives and social interactions has drawn researchers' attention to individual identity protection (Carter et al., 2020). In the mobile identity context, Mylonas et al. (2013) suggest that individuals may take several technical measures to protect their mobile identities according to their experience in mobile protection practices and security awareness. For instance, they present two levels of protection 1) the mobile pre-installed security controls (i.e., encryption, device password lock, remote data wipe, remote device locator) and 2) third-party security software (e.g., anti-virus, anti-theft software, etc.) for an additional line of defense against mobile identity threats. Most of the discussed technical-related solutions neglect the impact of the motivational aspects on an individual's protection behavior, especially in the mobile identity context.

2.3.3.2. The motivational aspects of protection. In the extant literature, research on motivational behavior examined the effect of motivation on individual protection behavior. For instance, Kominis and Emmanuel (2007) used EVT to develop an extended model of managerial motivation to measure the level of performance expected of managers and rewards associated with performance attainment. Recently, Sheffler et al. (2020) also used EVT to understand the relationship between badge reward design elements and ridership. In his research, he explored the efficacies of different badge designs of gamified applications in motivating ridership.

As suggested previously, the existing mobile security literature focuses mainly on the technical means of protection and neglects the impact of the motivational aspect of individuals' protection behavior, especially in the mobile identity context. For instance, Kraus, Wechsung, and Möller (2017) argue that protective behavior in the mobile context is not only dependent on a secure device and the implementation of security procedures but also on the users' motivations for applying security actions on their devices. Bélanger and Crossler (2019) suggest that it is important to not only measure protection intentions but also individuals' protective practices in the mobile security context. Hence, this study suggests that motivational aspects should not be treated separately from the technical means of protection.

2.3.3.3. The technical-motivation sources. Feather (1982) theorizes his motivational behavior model that emphasize an individual's perceived values. He suggests two main factors that motivate individuals to achieve a task - it must be important and have some value to them. The theory suggests that several factors influence the user's perceived value of mobile identity protection, such as achievement motivation which concerns self-enhancement; social motivation, which is concerned with peoples' influence and extrinsic and intrinsic motivations (Goodyear et al., 2004; Sclater and Bolander, 2004).

2.3.4. Protection awareness and experience

Vedadi and Warkentin (2020) suggest that when users are aware of the widespread use of a particular security technology, they develop a significantly higher intention to engage in protection-motivated behaviors. This description is consistent with Bulgurcu et al.'s (2010) definition of information security awareness, which refers to an "employee's general knowledge about information security and his cognizance of the ISP [information security policy] of his organization" (p. 532). Bulgurcu et al. differentiate between general information security awareness and security policy-specific awareness and the potential information security issues and their implications. In the mobile security context, identity protection awareness is defined as the protection experiences, capabilities, and motivation values expected by mobile users to understand mobile identity threats and the technical protection actions required to deal with them. It must, however, be noted that the context of mobile identity protection is different from the traditional well-researched organizational context unless mandated by a "bring your own device" policy.

Much information security research employed security awareness as an antecedent that explains motivation toward security behavior in the context of desktop computer security. For instance, Bulgurcu et al. (2010) suggest that information security awareness is an important driver that can restructure security education, training, and awareness programs and motivates employees to apply information security policies. Similarly, Kirova and Baumöl (2018) emphasize the significant role of information security awareness in enhancing security education training and awareness programs that guarantee end users are aware of security threats and motivate them to adhere to security policies. Donalds and Osei-Bryson (2020) recently showed that intrinsic and extrinsic motivation influence information security policy compliance. Their study used security awareness to predict individuals' security motivations and compliance behavior. In the mobile security context, researchers also use awareness as a predictor of mobile security motivational behavior (e.g., Allam et al., 2014; Mylonas et al., 2013). However, hardly any studies emphasize the mediating role of awareness in the mobile security context. In this regard, Wu et al. (2020) argue that a key issue in mobile security is that users have a serious lack of security awareness. As a result, they believe it is critical to identify mechanisms that can increase user mobile security awareness.

This study suggests that motivation can enhance individual information security awareness and consequently increase mobile identity protection intentions. Therefore, we examine the mediating impact on the relationship between individual protection motivation and intention toward mobile identity protection even though the extant literature does not explicitly state such to be the case. To ensure empirical grounding, our qualitative phase of the research explored the relationship in detail,

which eventually helped us develop our theoretical model (see Section 3).

Experience is the second construct that needs elaboration. Experience is related to individual abilities, knowledge, and skills, which are developed through formal or informal education (van Maele and van Houtte, 2012). Shen et al. (2011) referred to experience as the knowledge or skills people obtain through involvement in or exposure to a particular event. In the information security context, Safa et al. (2016) defined experience as individuals' familiarity with security incidents, skills, and the ability to prevent, manage, and mitigate the risk of security vulnerabilities. The lack of information security experience is one of the main factors that impact the role of individuals toward information security behavior (Albrechtsen, 2007).

While the moderating effect of user experience on behavioral intention and technology acceptance has been widely recognized as positive (e.g., Crespo et al., 2013; Lin, 2011; Shen et al., 2011, among others), this has not usually been the case for information security. However, while studying information security policy compliance, Bulgurcu et al. (2009) found work experience to have a significant moderating impact in strengthening the relationship between individual and organizational beliefs and information security policy compliance. This study explores the moderating role of protection experience on the intention to protect mobile identity.

In summary, although mobile security has been studied extensively over the years, most studies have focused on the role of individual protective capabilities ignoring their expectations in protecting their mobile identities. Past research has also either adopted a technical orientation towards protection or has exclusively relied on the motivational aspects. Finally, the majority of the studies have neglected the role of protection awareness and experience and the relationship between motivated users and their behavioral intentions toward mobile identity protection. Thus far, in the literature review section, we have explained these gaps and the related sources. As noted, there is some disagreement in the literature about the role of awareness and experience, as is the conceptualization of technical and motivational aspects. It is, therefore, essential to explore some of the relationships more substantively through qualitative in-depth case analysis.

3. Research design

3.1. The mixed-methods design

This study follows the guidelines of mixed methods research suggested by Venkatesh et al. (2013, 2016) to develop a conceptual model to understand the protection gaps in the mobile context. The purpose of conducting a mixed-methods design is to help develop the hypotheses and the conceptual model using the qualitative study results, given the lack of understanding of the role of motivation in mobile identity protection, and to examine the identity protection gaps resulting from the literature. Venkatesh et al. (2016) suggest that the objectives of conducting mixed methods research with a developmental purpose are multifold. Mixed methods allow for the use of results from one study to help develop or inform a subsequent study and increase the validity of constructs. This study follows Wunderlich et al.'s (2019) sequential mixed-methods design for developmental purposes. Table 1 summarizes the mixed-methods research approach in this study.

3.1.1. The qualitative study (Phase 1)

The qualitative in-depth phase is based on a Southern European bank. The case study aims to understand the mobile identity protection gaps. A bank has been chosen as a case study since financial institutions take identity management seriously, and much of banking now uses online mobile platforms. The purpose of the qualitative case study was threefold. First, to examine the relevance of the expectancy-value concept and interpretation of the protection gaps. Second, to ensure that the identified constructs and the related hypotheses were grounded in reality. The third is to develop the hypotheses and the research model. To do so, twenty-one individuals working in a regional bank in Southern Europe were interviewed. As shown in Appendix 3, we cluster the interviewees into three stakeholder groups (i.e., tellers, managers, and IT) to better understand the impact of experience and awareness based on the interview role, which reflects their technical capability. To avoid bias, we divided the interviewees' collected data equally between the two authors who were in charge of analyses, coding, and categorization. For example, each researcher was in charge of analyzing two customer-facing bankers, four IT professionals, and four managers. Access was granted to over 80 individuals across several branches and the regional headquarters. Nevertheless, the interviews were halted after 21 participants were interviewed, as theoretical saturation was achieved. As shown in Appendix 4, our open-ended questions were based on the interview protocol refinement suggested by Castillo-Montoya (2016). The case study was conducted in the spirit of Walsham's (1993) interpretative approach.

Table 1
The mixed-methods research approach conducted in this study.

Research Phase	Method	Objective	Procedure
Literature Review	Literature search	Identify literature gaps	An exhaustive review of the existing literature on mobile security behavior following Wunderlich et al. (2019)
Qualitative	In-Depth Interview	Model Development	Interpreting and codifying the sensitized data in the tradition of interpretive research and as operationalized in Califf et al. (2020). The results from the qualitative study were used to develop the hypothesis as advocated by Venkatesh et al. (2013)
Quantitative	Survey	Model Testing	Testing the research model developed in the qualitative study as operationalized by Wunderlich et al. (2019) and advocated by Venkatesh (2013).

The data was gathered through two rounds of interviews conducted between November 2019 and April 2020. Many of the interviews were in person. However, because of the coronavirus pandemic, interviews after March 2020 were conducted through Zoom platform. The interview procedure was divided into four stages: (1) aligning interview questions with research topics, (2) developing an inquiry-based discussion, (3) receiving input on interview protocols, and (4) conducting the interview protocol. The unit of interview analysis is divided into two sections, the expectancy-capability gap and the technical-motivational gap in protecting individual mobile identity and their interrelationships.

Our qualitative data analysis followed the codification and presentation schematic suggested by Wunderlich et al. (2019) and Miles and Huberman (1994). To this effect, we structured our interview analysis into a higher-level category of variables and emergent themes. In the process, we were guided by our reference theories. We also analyzed the data by interpreting what the respondents said and then reviewing the interpretations from our theoretical stance. We then translated our analysis into codes and categories, which helped in identifying emergent and related concepts. We were then able to link the themes to higher levels categories. We systematically created abstract categories and sub-categories (Appendix 5) while assigning labels and codes to similar multiple observations. Fig. 2 depicts a network model of our qualitative analysis and interpretation using a streamlined codes-to-theory model that codified our in-depth interview using a streamlined codes-to-theory scheme as suggested by Saldaña (2021). This model is used to create a network model. The modeling begins by transcending the "reality" of our collected data and progressing toward abstract concepts. The circles

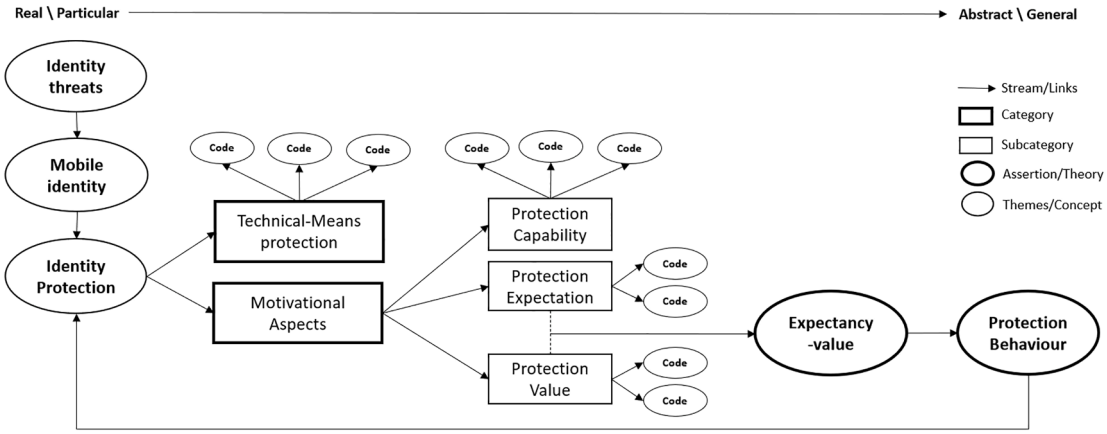

Fig. 2. A Network Model of the qualitative analysis.

represent the identified themes in reality. The rectangles represent the major categories and sub-categories that emerged from the interviews. Finally, the bold circles represent the interpreted concepts and theories. The network visualization for our codified qualitative data helped us to conclude and provided a basis for the subsequent phases of the study.

After reviewing the resulting translated transcripts and further analyzing the network representation for the identity protection context in the mobile environment, we identified three themes, two main categories, three sub-categories, and two theoretical concepts. We labeled the identified themes as identity threats, mobile identity, and identity protection. The identified two categories are technical means and motivational aspects of protection. We labeled the motivational aspects' subcategories as protection capability, protection expectation, and protection value. For the theories, we identified the expectancy-value theory (Eccles, 1983) and motivated protection behavior (Posey et al., 2013). Following other scholars (e.g., Sarker et al., 2002; Wunderlich et al., 2019), we used open coding in the coding and labeling process.

Several constructs can be gleaned from the initial coding, which can be linked to the identified categories, sub-categories, and concepts (Appendix 6). These include expectancy, capability, and related sources such as experience, vicarious experience, confidence, and protection importance. The extrinsic, intrinsic, social, and achievement motivation sources were viewed as strong predictors of the perceived value of mobile identity protection. Further, the technical and motivational protective actions were recurrently viewed. These themes are consistent with what was suggested in the literature. Based on the developed hypotheses shown in Appendix 6, we propose the conceptual model for mobile identity protection (Fig. 3). The model in Fig. 3 depicts the sources that explain the identified gaps. The dashed frames represent the expectancy-capability and technical-motivation gaps. The model also shows the moderation impacts of experience on protection gaps and intention toward mobile identity protection. Furthermore, the structural model highlights protection awareness as a mediator between identity protection gaps and mobile identity protection intention.

Given the aforementioned, we first explore the gaps and then test the mediation effect of protection awareness on the relationship between the examined gaps and the motivational protective intention. In the next section, we describe the quantitative study (Phase 2) that empirically tests our developed model to attain further depth and insight into the manifested gaps as well as the breadth of coverage of the motivated protection behavior in the mobile environment (Wunderlich et al., 2019).

3.1.2. *The quantitative part of the study (Phase 2)*

In this phase of our study, we empirically test the developed model resulting from the first phase of our mixed-methods research study. In this phase, we sought to examine the identity protection gap and explore the impact of motivation on the individual intention toward mobile

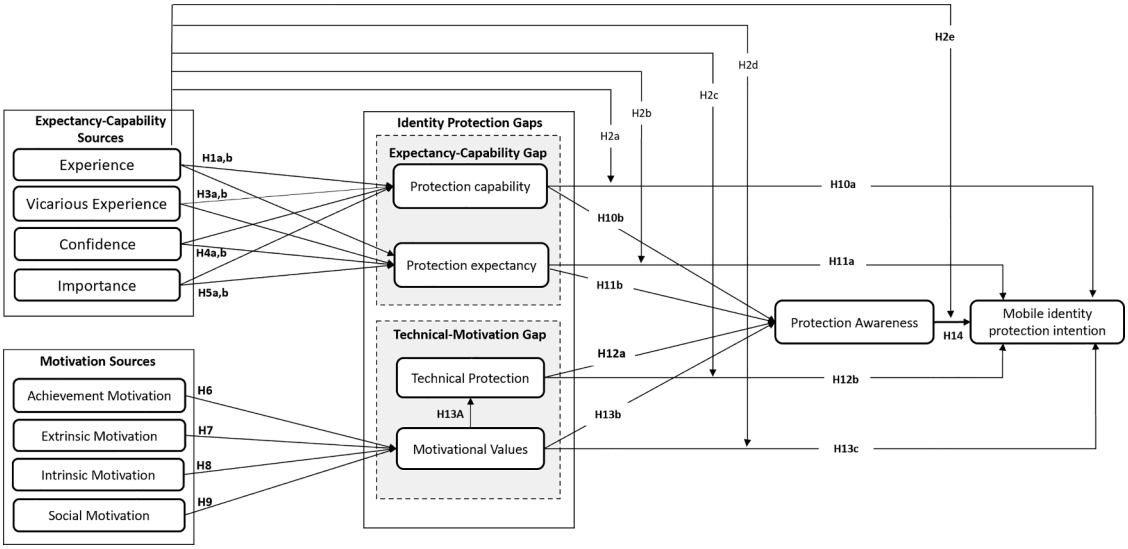

Fig. 3. The conceptual Model for mobile identity protection using EVT.

identity protection.

3.2.2.1. Participants. The respondents were 48% females, 52% males, and between 18 and 68 years. Most of them were highly educated (34% with a high school degree, 42% with a bachelor's degree, and 21% with post-graduate degrees), while only 3% had no school degree. 80% of the participants were from Europe, 13 % from the USA & Canada, and 7% from the rest of the world (Table 2).

3.1.2.2. Instrument development. To develop the measurement instrument of this study, we adopt an existing validated seven-point numerical scale. We adopted the new items and scales to fit our study context following the recommendations of MacKenzie et al. (2011) regarding the constructs measurements and valid procedures in IS behavioral research. We adapted the self-efficacy construct from Kim and Kankanhalli (2009) to measure the protection capabilities. Whereas protection expectancy items were adapted from the seminal work of Wigfield (1994) and Wigfield and Eccles (2000). The sources of the capability-expectancy gap include experience, which was adapted from Karahanna et al. (2006); confidence which was adapted from Wigfield and Eccles (2000), as well as confidence and importance, which was adapted from Wigfield and Eccles (2000), Wigfield (1994), and Eccles and Wigfield (1995) respectively.

To measure the motivational aspects, we adapted protection value from Trautwein et al. (2012); achievement motivation from Wigfield (1994); intrinsic motivation from Eccles and Wigfield (1995); extrinsic motivation from Eccles and Wigfield (1995), social motivation from Venkatesh et al. (2012) The technical protection actions were adapted from Chen and Zahedi (2016) and the mobile identity protection intention was adapted from the behavioral intention construct (Taylor and Todd 1995).

Later and based on the recommendations collected in the first qualitative phase of the study, we examined the mediation effect of protection awareness, which was adapted from Bulgurcu et al.'s (2010) study about information security awareness. The measurement instrument (Appendix 7) was validated using a panel of experts. We also conducted a pilot study before launching the actual data collection.

3.1.2.3. Data collection. In data collection, we used Prolific online data collection services. Prolific produces high data quality in terms of participants' attention, reliability, and reproducibility (Peer et al., 2017). Our data collection process started by conducting a pilot exploratory data collection for only 83 participants. The pilot reveals that the scales are reliable and valid. Thereafter, we surveyed 300 more respondents with a total of 383 responses. The published online survey took around 9–11 min, with an average of 10 min for each participant to finish the questionnaire.

We examined the common method bias (CMB) using two techniques. First, we used Harman's one-factor test to identify common method variance (Podsakoff et al., 2003). Second, we applied the PLS Marker variable approach to analyze data contaminated with method variance (Lindell and Whitney, 2001). The first method confirmed that none of the variables alone account for explaining most of the variance. While the latter had a maximum shared variance with other variables of 0.012 (1.2%), a number that could be considered (theoretically) as low and an irrelevant marker variable within the research model (Johnson et al., 2011). As a result, no substantial CMB was discovered.

3.1.2.4. Data analysis: measurement models. In this study, we use partial least squares (PLS) regression to conduct our analysis. Measurement models were used to test the construct reliability, convergent validity, indicator reliability, and discriminatory validity of scales for constructs in the two models. The constructs' reliability (CR) was tested using composite reliability. The results of CR were higher than 0.7 for all constructs (Table 3), which indicates the internal consistency and appropriateness of the constructs (Henseler et al., 2009; Straub, 1989).

The average variance extracted (AVE) was used to demonstrate convergent validity. The AVE quantifies the amount of variance captured by the constructs relative to measurement error, demonstrating that the observed indicators are indeed measuring the intended latent constructs accurately and reliably. As shown in Table 3, the AVE is larger than 0.50 for all constructs. As a result, the measurement model's convergent validity is established (Fornell and Larcker, 1981; Hair et al., 2012).

The analysis of loadings and cross-loadings is of paramount importance in assessing the reliability and discriminant validity of indicators. The loading should be greater than 0.7 to ensure indicator reliability (Churchill Jr, 1979; Henseler et al., 2009). By examining the magnitude of loadings, researchers can evaluate the strength of the relationships between the indicators and their respective latent constructs. Additionally, scrutinizing cross-loadings helps ensure that the indicators primarily reflect their intended constructs and not unrelated factors, thus establishing the discriminant validity of the measurement model. In this study, Table 4 demonstrates that all loadings surpass the 0.7 thresholds, indicating indicator reliability, while the bolded loadings outnumber the cross-loadings, further confirming the robustness of the measurement model.

The Heterotrait-Monotrait (HTMT) ratio of correlations is a widely used method for assessing discriminant validity among constructs. By comparing the correlations between different constructs to the correlations within the same construct, researchers can determine whether the constructs are distinct from one another (Henseler et al., 2009). Table 5 reveals that all HTMT values are below the recommended threshold of 0.9, indicating strong discriminant validity among the constructs. This implies that the constructs are sufficiently different from each other, ensuring that the measurement model accurately captures the unique variance associated with each construct which supports the validity of the study's measurement model and reinforces confidence in the interpretations of construct relationships and effects in subsequent analyses.

3.1.2.5. The structural model. Using the variance inflation factor (VIF), we investigated the multicollinearity of all constructs. The VIF is 1.67, which is less than the threshold of 3.3, indicating that the variables are not multicollinear (Lee and Xia, 2010). Fig. 4 presents the structural model that explains the variation and path coefficients. Both significant and insignificant paths are shown through solid and dashed lines, respectively.

Table 2
Profile of the respondents.

Characteristics	(%)	n = 383	Avg	STD		Characteristics		(%)	n = 383
Age	18–24	43%	163	21.3	1.842	**Educational Degree**	No school	3%	11
	25–34	31%	120	28.7	2.730		High School	34%	130
	35–44	15%	59	38.8	3.276		Bachelor	42%	160
	45–54	7%	25	48.4	2.972		Master	19%	73
	55–64	3%	12	58.4	3.476		Ph.D.	2%	9
	65–74	1%	4	67.7	2.500	**Gender**	Female	48%	185
							Male	52%	198

Table 3
Descriptive statistics, correlation, composite reliability (CR), and average variance extracted (AVE).

Construct	Mean	SD	CR	Exp	VExp	Conf	Imp	PC	PE	AM	EM	IM	SM	MV	TP	PA	MIPI
Experience (Expr)	3.656	1.814	0.929	**0.875**													
Vicarious experience (VExp)	3.570	1.679	0.936	-0.132	**0.823**												
Confidence (Conf)	4.338	1.435	0.936	-0.474	0.277	**0.888**											
Importance (Imp)	4.967	1.501	0.954	-0.301	0.241	0.441	**0.915**										
Protection capability (PC)	4.587	1.650	0.940	-0.447	0.256	0.736	0.331	**0.916**									
Protection expectancy (PE)	4.878	1.328	0.943	-0.347	0.260	0.776	0.535	0.691	**0.920**								
Achievement motivation (AM)	3.803	1.892	0.825	-0.146	0.284	0.246	0.606	0.160	0.398	**0.839**							
Extrinsic motivation (EM)	4.689	1.500	0.889	-0.150	0.213	0.348	0.687	0.251	0.441	0.604	**0.853**						
Intrinsic motivation (IM)	4.257	1.525	0.900	-0.254	0.286	0.491	0.651	0.361	0.542	0.527	0.561	**0.866**					
Social Motivation (SM)	4.371	1.700	0.938	-0.145	0.311	0.259	0.507	0.180	0.328	0.444	0.440	0.433	**0.914**				
Motivation Values (MV)	4.826	1.204	0.891	-0.094	0.135	0.339	0.443	0.282	0.449	0.415	0.492	0.422	0.377	**0.819**			
Technical Protective (TP)	4.530	1.606	0.935	-0.221	0.194	0.408	0.717	0.267	0.477	0.558	0.630	0.744	0.385	0.396	**0.910**		
Protection awareness (PA)	4.993	1.492	0.928	-0.311	0.186	0.544	0.448	0.500	0.604	0.337	0.429	0.424	0.383	0.428	0.403	**0.900**	
Mobile identity protection intention (MIPI)	5.686	1.305	0.906	-0.237	0.164	0.311	0.629	0.294	0.449	0.457	0.510	0.534	0.397	0.447	0.581	0.492	**0.874**

Notes: Values in diagonal (bolt) are the AVE square root; standard deviation (SD).

Bootstrapping with 5000 resamples was used to determine the statistically significant levels of the hypothesized constructs.

Individual capability to protect their mobile identity is explained by 56 %, and 65 % of users' expectancy to succeed in mobile identity protection is explained in the research model. *The individual's experience* was statistically significant for explaining protection capability ($\widehat{\beta}$= -0.128; $p < 0.01$), Its effect on protection expectancy is not statistically significant. ($\widehat{\beta}$= 0.055; $p > 0.01$). Hence, H1a is supported, and H1b is not supported.

The moderating effect of users' experience on the relationship between 1) expectancy and identity protection motivation intention is confirmed ($\widehat{\beta}$=- 0.106; $p < 0.01$); 2) protection values and identity protection motivation intention is confirmed ($\widehat{\beta}$= 0.136; $p < 0.01$); 3) protection awareness and mobile identity protection are also confirmed ($\widehat{\beta}$= -0.098; $p < 0.01$). Hence H2b, H2d, and H2e are supported. However, users' experience moderation effect is not statistically significant in explaining the relationship between 1) the protection capability and mobile identity protection intention ($\widehat{\beta}$= -0.039; $p > 0.1$), and 2) the technical protection and mobile identity protection intention ($\widehat{\beta}$= -0.024; $p > 0.1$). Hence, H2a and H2c are not supported.

Vicarious experience is statistically significant for predicting protection capability ($\widehat{\beta}$= 0.060; $p < 0.1$) and not statistically significant to explain protection expectancy ($\widehat{\beta}$= 0.008; $p > 0.017$). Thus, H3a is supported, and H3b is not supported.

The individual's confidence is statistically significant for explaining both the protection capability ($\widehat{\beta}$= 0.666; $p > 0.01$) and statistically significant in explaining protection expectancy ($\widehat{\beta}$= 0.691; $p > 0.01$). Thus, hypotheses H4a and H4b are supported.

The protection importance is not statistically significant in explaining protection capability ($\widehat{\beta}$= -0.015; $p > 0.01$) and is statistically significant for explaining protection expectancy ($\widehat{\beta}$= 0.243; $p < 0.01$). Thus, hypotheses H5a and H5b are supported.

The research model explains 16 % of technical protective actions and 63 % of mobile identity protection value. Achievement motivation ($\widehat{\beta}$= 0.123; $p < 0.01$), extrinsic motivation ($\widehat{\beta}$= 0.260; $p < 0.01$) and intrinsic motivation ($\widehat{\beta}$= 0.541; $p < 0.01$) are statistically significant for explaining mobile identity protection value. However, the hypothesis of social motivation is not statistically significant ($\widehat{\beta}$= -0.018; $p > 0.1$) in explaining mobile identity protection value. Also, protection values ($\widehat{\beta}$= 0.337; $p < 0.01$) is statistically significant in explaining technical protection. Hence, H6, H7, H8, and H13a are supported while H9 is not supported.

The model also explains 43 % of users' mobile identity protection intention. While the hypothesis about protection expectancy ($\widehat{\beta}$= 0.102; $p < 0.01$) was found to be statistically significant in explaining the mobile identity protection intentions, the protection capability of mobile users was not statistically significant ($\widehat{\beta}$= 0.024; $p > 0.1$), i.e., the expectancy-capability gap exists. On the other hand, both the technical protection ($\widehat{\beta}$= 0.170; $p < 0.01$), and protection values ($\widehat{\beta}$= 0.337; $p < 0.01$) are statistically significant to explain mobile identity protection intention, i.e., the technical motivation gap does not exist. Thus, H10a is not supported, and H11a, H12, and H13b are supported.

As predicted, our measurements show that the expectancy-capability gap exists (i.e., the individuals' capabilities do not match their expectations). Our qualitative analysis suggests that the main cause of this gap is a lack of awareness about the new identity theft techniques and the appropriate protective behavior. To resolve this incongruence, we examine the impact of awareness as a mediator variable on the relationship between the expectancy-capability gap and mobile identity protection intentions. The structural model explains 37 % of the protection awareness. The research model shows that both the hypotheses

Table 4
Loadings and cross-loadings.

Construct	Items	Expr	VExp	Conf	Imp	PC	PE	AM	EM	IM	SM	MV	TP	PA	MIPI
Experience (Expr)	Expr1	**0.875**	-0.181	-0.462	-0.320	-0.439	-0.363	-0.136	-0.146	-0.267	-0.173	-0.050	-0.216	-0.318	-0.211
	Expr2	**0.907**	-0.097	-0.410	-0.288	-0.381	-0.322	-0.162	-0.160	-0.228	-0.110	-0.105	-0.234	-0.295	-0.234
	Expr3	**0.893**	-0.080	-0.408	-0.274	-0.375	-0.285	-0.139	-0.153	-0.232	-0.128	-0.105	-0.219	-0.259	-0.205
	Expr4	**0.823**	-0.093	-0.368	-0.151	-0.361	-0.227	-0.064	-0.055	-0.148	-0.087	-0.071	-0.086	-0.203	-0.174
Vicarious experience (VExp)	VExp1	-0.176	**0.839**	0.294	0.196	0.256	0.266	0.261	0.181	0.196	0.220	0.130	0.168	0.166	0.128
	VExp2	-0.120	**0.838**	0.213	0.163	0.236	0.199	0.242	0.155	0.207	0.199	0.064	0.167	0.124	0.126
	VExp3	-0.047	**0.731**	0.191	0.178	0.172	0.152	0.143	0.136	0.210	0.295	0.064	0.074	0.150	0.044
	VExp4	-0.133	**0.771**	0.244	0.263	0.247	0.255	0.219	0.190	0.280	0.336	0.146	0.126	0.225	0.152
	VExp5	-0.086	**0.877**	0.196	0.185	0.161	0.190	0.208	0.161	0.225	0.260	0.094	0.172	0.111	0.155
	VExp6	-0.072	**0.865**	0.202	0.180	0.172	0.195	0.241	0.197	0.230	0.259	0.105	0.176	0.148	0.182
Confidence (Conf)	Conf1	-0.460	0.266	**0.920**	0.439	0.706	0.718	0.232	0.356	0.450	0.261	0.369	0.386	0.516	0.316
	Conf2	-0.368	0.303	**0.880**	0.418	0.647	0.630	0.227	0.351	0.429	0.263	0.271	0.348	0.481	0.232
	Conf3	-0.430	0.169	**0.863**	0.316	0.607	0.717	0.196	0.219	0.429	0.166	0.257	0.351	0.450	0.275
Importance (Imp)	Imp1	-0.291	0.214	0.408	**0.909**	0.313	0.503	0.574	0.639	0.613	0.476	0.419	0.665	0.441	0.564
	Imp2	-0.264	0.236	0.388	**0.915**	0.296	0.475	0.547	0.639	0.602	0.487	0.397	0.660	0.396	0.570
	Imp3	-0.278	0.236	0.411	**0.929**	0.323	0.508	0.558	0.634	0.579	0.459	0.405	0.638	0.408	0.601
	Imp4	-0.268	0.194	0.405	**0.907**	0.276	0.471	0.537	0.602	0.588	0.433	0.396	0.665	0.395	0.565
Protection Capability (PC)	PC1	-0.351	0.200	0.652	0.273	**0.890**	0.640	0.153	0.214	0.330	0.188	0.252	0.248	0.513	0.270
	PC2	-0.431	0.243	0.672	0.299	**0.924**	0.598	0.132	0.240	0.304	0.152	0.258	0.229	0.425	0.273
	PC3	-0.447	0.262	0.699	0.337	**0.934**	0.660	0.154	0.237	0.357	0.155	0.264	0.255	0.437	0.265
Protection Expectancy (PE)	PE1	-0.363	0.223	0.785	0.460	0.678	**0.922**	0.348	0.398	0.504	0.311	0.420	0.439	0.556	0.379
	PE2	-0.284	0.243	0.670	0.478	0.599	**0.918**	0.382	0.412	0.492	0.271	0.420	0.426	0.572	0.413
	PE3	-0.311	0.250	0.687	0.539	0.630	**0.922**	0.370	0.407	0.500	0.323	0.401	0.453	0.540	0.450
Achievement motivation (AM)	AM1	-0.101	0.248	0.177	0.441	0.140	0.313	**0.777**	0.485	0.402	0.375	0.338	0.379	0.274	0.350
	AM2	-0.140	0.235	0.230	0.564	0.132	0.354	**0.896**	0.530	0.478	0.377	0.362	0.538	0.293	0.414
Extrinsic motivation (EM)	EM1	-0.181	0.150	0.361	0.657	0.306	0.450	0.536	**0.892**	0.530	0.385	0.470	0.634	0.421	0.512
	EM2	-0.127	0.182	0.312	0.588	0.205	0.376	0.521	**0.879**	0.479	0.373	0.405	0.529	0.373	0.440
	EM3	-0.053	0.234	0.187	0.491	0.092	0.272	0.489	**0.784**	0.412	0.374	0.374	0.417	0.282	0.323
Intrinsic motivation (IM)	IM1	-0.231	0.278	0.434	0.524	0.310	0.467	0.441	0.446	**0.837**	0.336	0.323	0.639	0.338	0.408
	IM2	-0.230	0.235	0.400	0.580	0.299	0.458	0.480	0.496	**0.900**	0.429	0.422	0.652	0.399	0.513
	IM3	-0.200	0.229	0.443	0.585	0.328	0.482	0.448	0.515	**0.859**	0.358	0.348	0.641	0.365	0.464
Social motivation (SM)	SM1	-0.132	0.302	0.243	0.459	0.193	0.327	0.413	0.401	0.369	**0.914**	0.350	0.355	0.376	0.382
	SM2	-0.104	0.255	0.210	0.457	0.118	0.263	0.409	0.404	0.392	**0.905**	0.352	0.360	0.332	0.348
	SM3	-0.164	0.294	0.258	0.473	0.184	0.311	0.395	0.402	0.426	**0.922**	0.329	0.341	0.342	0.359
Motivation Values (MV)	MV1	-0.085	0.098	0.294	0.413	0.239	0.430	0.430	0.455	0.355	0.356	**0.833**	0.377	0.425	0.393
	MV2	-0.121	0.109	0.267	0.353	0.249	0.347	0.304	0.376	0.315	0.297	**0.829**	0.270	0.331	0.349
	MV3	-0.006	0.101	0.177	0.296	0.140	0.238	0.289	0.348	0.330	0.268	**0.777**	0.287	0.237	0.337
Technical Protective (TP)	TP1	-0.085	0.133	0.351	0.371	0.280	0.423	0.318	0.418	0.377	0.302	**0.836**	0.346	0.380	0.379
	TP2	-0.140	0.194	0.344	0.581	0.175	0.406	0.492	0.550	0.665	0.303	0.355	**0.886**	0.322	0.482
	TP3	-0.211	0.147	0.348	0.699	0.251	0.443	0.518	0.579	0.658	0.349	0.372	**0.909**	0.391	0.572
	TP4	-0.248	0.190	0.420	0.673	0.297	0.453	0.512	0.590	0.709	0.397	0.353	**0.934**	0.384	0.528
Protection awareness (PA)	PA1	-0.266	0.157	0.468	0.417	0.418	0.548	0.329	0.390	0.390	0.389	0.361	0.378	**0.900**	0.461
	PA2	-0.351	0.179	0.531	0.338	0.481	0.542	0.260	0.341	0.362	0.327	0.359	0.300	**0.887**	0.378
	PA3	-0.232	0.168	0.474	0.451	0.455	0.542	0.316	0.422	0.393	0.320	0.434	0.405	**0.913**	0.483
Mobile identity protection intention (MIPI)	MIPI	-0.236	0.179	0.356	0.641	0.278	0.465	0.498	0.545	0.576	0.416	0.456	0.614	0.471	**0.901**
	MIPI2	-0.148	0.074	0.153	0.390	0.254	0.308	0.254	0.269	0.251	0.227	0.302	0.307	0.363	**0.783**
	MIPI3	-0.220	0.155	0.264	0.570	0.243	0.379	0.398	0.466	0.502	0.361	0.388	0.537	0.441	**0.931**

about protection capability ($\widehat{\beta}$= 0.178; p < 0.01) and protection expectancy ($\widehat{\beta}$= 0.469; p < 0.01) were found to be statistically significant in explaining protection awareness. Hence, H10b and H11b are supported. Protection awareness was also found to be statistically significant in explaining mobile identity protection intentions ($\widehat{\beta}$= 0.223; p < 0.01). Hence, H14 is also supported.

3.1.2.6. Mediation results in awareness. As predicted, our measurements show that the expectancy-capability gap exists (i.e., the individuals' capabilities do not match their expectations). We suggest that the leading cause of this gap is a lack of awareness about the new identity theft techniques and the appropriate protective behavior. Therefore, we analyzed the mediation impact of awareness to understand more about the protection motivation gaps. To assess the mediating variables and estimate the indirect effect of our model, we used MacKinnon (2008) product of a coefficient approach. As shown in Table 6, the structural model shows that while awareness has a complementary mediation impact on the relationship between expectations and individuals' protection intention, it has a full mediation impact on the relationship between protection capability and protection intention toward mobile identity protection. The mediation results indicate that protection awareness plays a significant role in bridging the gap between individuals' misperceptions about their expectations to protect their

Table 5
Heterotrait-monotrait ratio (HTMT).

Construct	Expr	VExp	Conf	Imp	PC	PE	AM	EM	IM	SM	MV	TP	PA	MIPI
Experience (Expr)														
Vicarious experience (VExp)	0.135													
Confidence (Conf)	0.532	0.303												
Importance (Imp)	0.322	0.255	0.489											
Protection Capability (PC)	0.493	0.272	0.831	0.359										
Protection Expectancy (PE)	0.377	0.275	0.873	0.580	0.761									
Achievement motivation (AM)	0.192	0.384	0.339	0.804	0.221	0.542								
Extrinsic motivation (EM)	0.162	0.253	0.400	0.776	0.274	0.498	0.869							
Intrinsic motivation (IM)	0.289	0.326	0.579	0.738	0.416	0.623	0.746	0.674						
Social Motivation (SM)	0.159	0.341	0.294	0.552	0.200	0.362	0.613	0.515	0.499					
Motivation Values (MV)	0.113	0.150	0.387	0.493	0.318	0.502	0.581	0.584	0.502	0.429				
Technical Protective (TP)	0.239	0.213	0.462	0.782	0.294	0.528	0.750	0.721	0.862	0.427	0.450			
Protection Awareness (PA)	0.348	0.201	0.623	0.490	0.561	0.674	0.465	0.493	0.494	0.430	0.485	0.449		
Mobile identity protection intention (MIPI)	0.262	0.178	0.342	0.684	0.337	0.500	0.614	0.572	0.602	0.437	0.514	0.636	0.558	

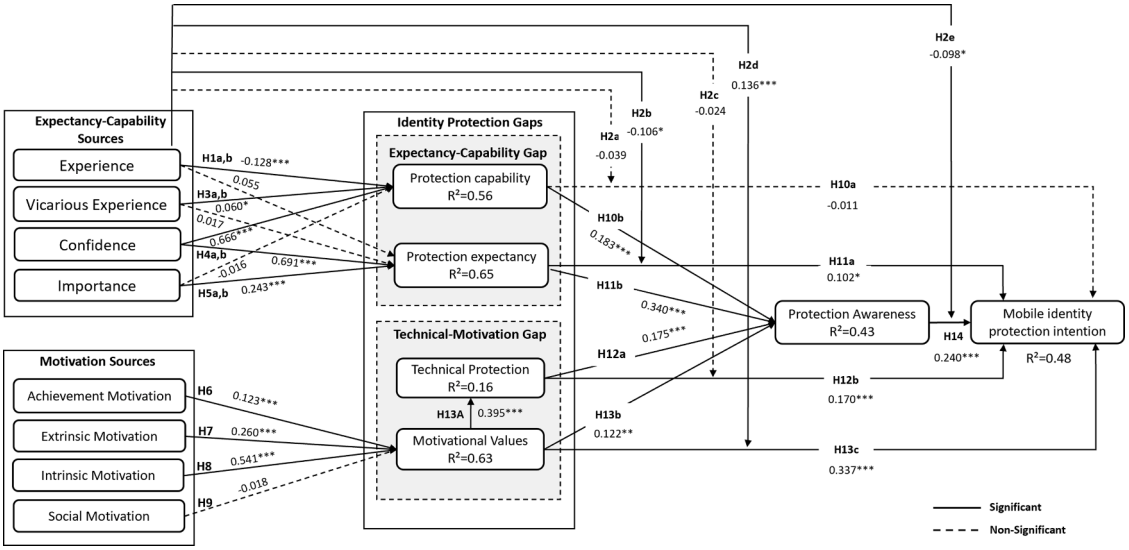

Fig. 4. The structural model
Notes: *** p < 0.01; ** p < 0.05; * p < 0.10.

Table 6
The mediation analysis.

Independent Variable (IV)	Mediator (M)	Dependent Variable (DV)	Direct Effect	Indirect Effect (Product of Coefficients)			Mediating Effect
			IV → DV (C)	IV → M (A)	M → DV (B)	IV → M→ DV (A x B)	
Expectancy	Awareness	Protection Intention	0.102*	0.340***	0.240***	0.081**	Complementary Mediation
Capability			-0.011	0.189***		0.045**	**Full Mediation**
Technical Actions			0.170***	0.175***		0.042**	Complementary Mediation
Motivation Values			0.337***	0.122**		0.029**	

mobile identity and their capabilities. The results also show the complementary mediation impact of awareness on technical action and mobile identity protection intentions from one side and motivational values and intentions toward mobile identity protection from the other side. These results show the importance of protection awareness in enhancing both technical and motivational means of protection against mobile identity protection.

4. Discussion of the Results

Belanger et al. (2019) identified the growing concern over unintentional information leakage due to the increasing use of mobile devices in organizations. In the same context, Hedström et al. (2011) emphasized the strategic importance of information values as essential assets for organizations. However, Feather (1982) noted that motivational theories that used perceived values to explain individual behavior fail to connect cognition and action, highlighting a critical issue in understanding human behavior. According to Feather, the lack of a clear link between cognition and action leaves individuals "buried in thoughts," unable to translate their values and intentions into effective action. To address this problem, Feather suggested using the "expectancy-value approach."

This study use EVT as a conceptual framework. We employ a mixed-methods approach to investigate the gap between individuals' expectations and capabilities in mobile identity protection and the role that motivation plays in predicting individual behavior. This study is the first to investigate the expectancy-capability gap in the context of mobile identity protection.

The theoretical contributions of this study can be classified into four main areas. Firstly, our results suggest that an individual's protection

awareness mediates the relationship between expectancy-capability and individuals' protection intentions. This finding highlights the existence of a gap between individual expectations and their actual capabilities to protect their mobile identity. Secondly, the motivational aspects of identity protection values significantly influence an individual's intention toward mobile identity protection. Specifically, achievement and intrinsic and extrinsic motivations are the determinant factors that explain the motivational aspect of mobile identity protection values. Finally, the study shows the significant moderation role of experience in moderating the individuals' expectations and protection values from one side and their protection intentions from the other side.

4.1. Why do expectations fail?

The results of our study indicate that individual protection capability does not affect the intention to protect mobile identity. On the other hand, individual expectations about identity protection have a significant impact on identity protection intention. Therefore, predicting mobile users' intentions to protect their identity fails because individuals cannot identify or perceive their protection capabilities relative to their false expectations. When comparing our findings to the extant literature on mobile identity protection in the context of mobile security, important questions arise. Firstly, to what extent does prior research overlook user expectations as a key element in predicting individual protection behavior by focusing only on protection capabilities in the mobile environment?. Secondly, how much does the lack of protection awareness impact the expectancy-capability gap?

The literature review section and Appendix 1 highlight the gap where the extant literature does not specifically study user expectations regarding their protection behavior. Researchers have focused more on the role of individual capability in explaining protective behaviors. Studying the impact of both individual protective expectations and perceived capabilities contributes to providing clearer insight into individual protection behavior and, more specifically, into the discrepancy emerging from the expectancy-capability gap.

Individual beliefs about protection capabilities could be confused with their judgments of the protection outcomes that they expect. This argument was originally made by Bandura (1986). He argued that individual outcome expectations are unlikely to lead to behavioral forecasts since the results they expect are the product of individual expectations of what they can achieve. In psychology, the same concept was explained by Higgins (1987) when proposing the self-discrepancy theory. He argued that individuals compare their actual self to the ideal or ought self. The expectancy-capability gap is the gap between the actual self (i.e., the ideal version of yourself created from experience) and the ideal or ought self (i.e., the expectations of persons who feel they should become or should achieve).

Regarding the sources that explain the expectancy-capability gap, the results show that while user experiences and vicarious experiences significantly impact protection capabilities, they do not impact expectations. Confidence significantly impacts both individual capabilities and expectations to protect their mobile identity. Mobile identity protection's perceived importance is found to significantly impact individual expectations but not their protection capabilities.

Bandura et al. (1999) suggest that individual expectations are unlikely to make much of an independent contribution to predicting behavior when perceptions about individual capabilities are controlled. This rational explanation of the expectancy-capability gap led us to address the role of awareness in explaining the protection behavior of individuals in a mobile environment. Our results show that individual awareness affects their intention to achieve mobile identity protection. Prior research has shown that individuals who lack awareness of smartphone security issues exercise ineffective or a lack of protective behaviors. In the same vein, user awareness of the threats posed by negative technologies like spyware strongly predicts user behavioral intention to use protective technologies.

The present study offers a significant contribution to the existing literature by shedding new light on the perception of mobile user protective behaviors. Specifically, the findings highlight the critical role of discrepancy perception in this regard, which captures the divergence between individuals' expectations and their actual abilities to safeguard their mobile identities. This notion not only advances our theoretical understanding of the protective behavior literature but also has practical implications for the development of effective interventions.

Moreover, the study results underscore the importance of protection awareness as a potential solution for addressing this discrepancy effectively. By enhancing individuals' knowledge and understanding of the threats to their mobile identities, such interventions can help bridge the gap between expectations and capabilities, thereby promoting more effective protective behaviors. In doing so, protection awareness can serve as a powerful tool for safeguarding individual mobile identities in an increasingly interconnected and vulnerable digital landscape. In conclusion, this study underscores the importance of understanding the role of the expectancy-capability gap in predicting individual protective behavior, particularly in the mobile environment. The study findings suggest that increasing individuals' protection awareness and understanding the motivational aspects of identity protection values can enhance their intention to protect their mobile identity. This study provides valuable insights for organizations seeking to improve their mobile security policies and practices, as well as for individuals seeking to protect their mobile identities.

4.2. Technical or motivational protection?

This study explores the complex relationship between technical and motivational means of protecting mobile identities. While our initial hypothesis suggested a technical-motivation gap, our findings reveal that the perceived value of mobile identity protection significantly influences individual protective behaviors. In particular, motivation protection emerges as the stronger determinant in explaining such behaviors in the mobile context. Our study results further suggest that the perceived value of mobile identity protection is significantly affected by a user's achievement motivation and intrinsic, and extrinsic motivation.

The extant literature provides insight into the intricate nature of motivation and its impact on perceived value. Specifically, individual achievement motivation and extrinsic motivation or utility value significantly influence the perceived value of required tasks, such as protecting mobile identity using dual-factor authentication. Notably, social motivation appears to have no significant effect on the perceived value of mobile identity protection, despite its critical role in shaping individual behaviors in a wide variety of domains. From a social motivation perspective, social influence may impact the perception of value. Overall, our study findings contribute a novel understanding of the complex factors that shape mobile identity protection behaviors and suggest potential avenues for bridging the gap between protective behaviors and actual capabilities.

4.3. The moderation effect of the user's experience

The importance of prior experience on current behavior toward a task has been extensively discussed in the literature (Ajzen and Fishbein, 1975). As such, individuals who have successfully engaged in a particular task in the past are more likely to possess the knowledge and skills required to accomplish the same task in the future. Conversely, individuals attempting a new task for the first time may experience heightened anxiety levels, as their expectations for success are uncertain (Sclater and Bolander, 2004).

In examining the role of user experience in mobile identity protection, our study reveals that low-experienced users' expectations play a significant role in explaining their motivational intentions toward achieving mobile identity protection. Specifically, low-experienced

users with high expectations to succeed in mobile identity protection are more motivated to achieve protection than low-experienced users with low expectations (Fig. 5). Moreover, low-experienced users who value mobile identity protection have a higher motivational intention to protect their mobile identity. Conversely, low-experienced users who perceive low value in mobile identity protection exhibit lower motivational intentions toward protecting their mobile identity (Fig. 6).

Our findings also indicate that protection awareness is an essential predictor of identity protection motivational intention for low-experienced users. Low-experienced users with low levels of protection awareness exhibit lower motivational intentions to achieve mobile identity protection than those with high levels of protection awareness (Fig. 7). Taken together, our results suggest that the role of user experience, protection awareness, and value are important factors that determine motivational intentions toward mobile identity protection.

The findings of this study have important implications for developing effective training programs aimed at improving mobile identity protection among low-experienced users. The moderation effect of experience suggests that training programs need to be tailored to the specific needs of low-experienced users, focusing on improving their expectations and perceived values regarding mobile identity protection. To achieve this, companies could implement gamified training programs that provide incentives and rewards for achieving protection goals, thereby increasing trainees' extrinsic motivation and protection awareness. By doing so, these programs could successfully bridge the technical-motivation gap that often exists in mobile identity protection, leading to improved protective behavior among low-experienced users. This approach has potential applications in a range of domains, as gamified training programs could be adapted to target low-experience employees across a variety of industries. Overall, this study offers a novel approach to improving mobile identity protection and highlights the importance of tailored training programs in promoting protective behavior among low-experienced users.

Companies that rely on mobile applications should prioritize their efforts toward users who are inexperienced in protecting their mobile identities. To do this, they should emphasize the importance and value of mobile identity protection and focus on increasing user self-confidence and awareness. By improving individual expectancy, users will be more motivated to protect their mobile identities. Additionally, companies should encourage their customers to use multi-factor authentication, specifically biometric authentication using their mobile devices. For instance, banks could reward their customers for installing mobile banking applications on their smartphones or tablets and take advantage of embedded authentication technologies such as fingerprints and facial recognition. This extrinsic motivation technique would heighten identity protection and deter fraudsters.

In conclusion, user experience is one of the most significant factors in mobile identity protection. It motivates mobile users' attitudes towards identity protection, increases their expectations of success in protecting their identities, improves their perception of the value of mobile identity protection, and strengthens the relationship between protection awareness and users' intention towards mobile identity protection. Companies that prioritize these factors will have a better chance of promoting mobile identity protection among their customers and employees.

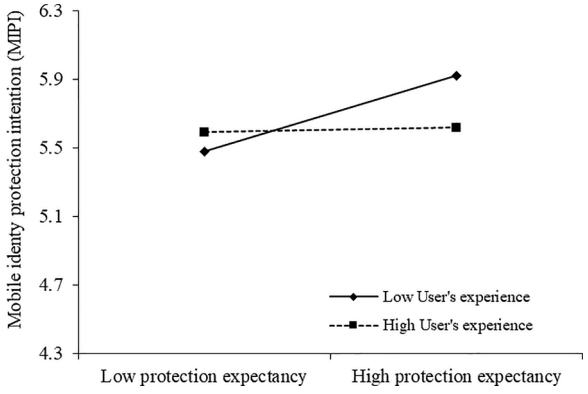

Fig. 5. The moderation effect of user's experience on the relation between protection expectancy and mobile identity protection intention.

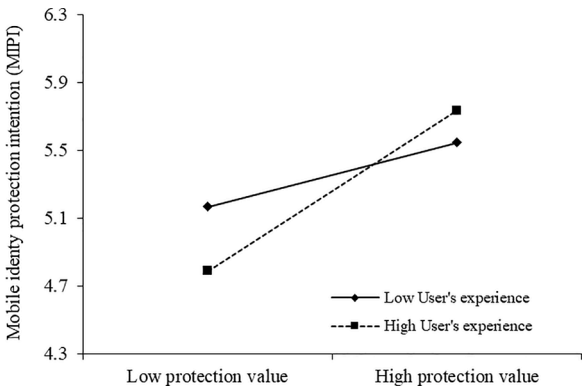

Fig. 6. The moderation effect of user's experience on the relation between protection value and mobile identity protection intention.

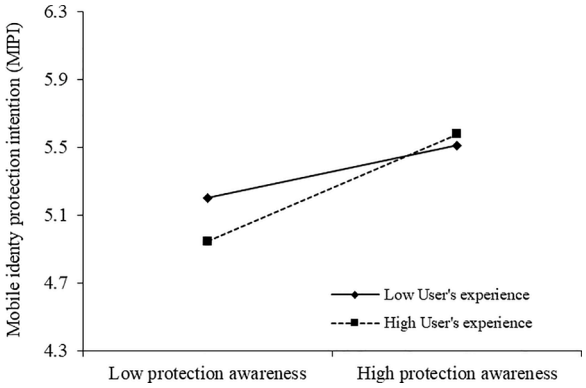

Fig. 7. The moderation effect of user's experience on the relation between protection awareness and mobile identity protection intention.

5. Limitations and future work

During the study, the limitations found were mainly concerned with the validation of our findings, specifically with the moderation effect of experience, which may lead to future lines of research. Accordingly, a panel of mobile security experts and mobile users may be considered in the future to validate the findings of this study. The outcome of this study can be applied to further specific research, which focuses on different domains such as digital marketing and e-learning using the ubiquitousness of mobile devices as a new digital identity for consumers and students. Furthermore, control variables could also be applied to studies such as geography, gender, and education, among others, to examine their impact on mobile users' intentions toward identity protection. Furthermore, the mobile identity threats construct (Craig et al., 2019) could be added to our model to examine the effect of identity threats as a stimulus on mobile users and how it could motivate their responses toward mobile identity protection. Finally, in light of the escalating threats of identity theft and related attacks in the mobile environment, it is highly suggested to prioritize the adoption of anonymization methods. Conducting future research to explore the integration of anonymization techniques in mobile identity protection becomes a crucial agenda. By implementing data anonymization

techniques, such as the combined utilization of semantic properties and generalization, as Caruccio et al. (2022) suggested, the privacy and confidentiality of mobile users' personally identifiable information (PII) can be effectively safeguarded. This approach may not only mitigate the risk of unauthorized access but may also reduce the possibility of re-identification, ensuring the utmost security of mobile identity data.

6. Conclusion

The findings of our study underscore the importance of individual awareness and motivation in protecting mobile identity against potential threats such as identity theft and cyberattacks. We have identified that a gap often exists between individuals' expectations and their actual capabilities in safeguarding their mobile identity, resulting in an expectancy-capability gap. To address this gap, increasing employee awareness about mobile identity protection in the workplace is essential. Our research suggests that technical measures alone are insufficient to address the challenges of identity theft and associated threats. Motivating employees to prioritize mobile identity protection can enhance their technical protective actions. Furthermore, our study demonstrates the significant impact of experience on an individual's expectations, capabilities, and values toward mobile identity protection. Therefore, organizations should prioritize increasing employee awareness about the importance of mobile identity protection and provide regular training and resources to help employees safeguard their mobile identities in the workplace. By taking these steps, organizations can effectively prevent potential cyberattacks and identity theft that may compromise sensitive data and harm business operations. Our study highlights the crucial role of employee awareness and motivation in ensuring the security of mobile identities and emphasizes the need for organizations to prioritize this aspect of cybersecurity to achieve effective protection against potential threats.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

The authors do not have permission to share data.

Appendix

Appendix 1. The protection gaps in the mobile security literature

Protection Literature			Protection Concepts		Current Research Emphasis			Protection Gaps			
								Gap1		Gap2	
Authors	Context	findings	Theories	Constructs	Info/ Privacy Protection	Software Protection	Identity protection	Expectancy	Capability	Technical	Motivation
Rodriguez-Priego et al. (2022)	Mobile privacy protection	Privacy protection measures have no significant impact on privacy protection intention	PMT	Threat susceptibility; Threats vulnerability; Self-efficacy; Response, behavioral intention;	√				√		√
Ameen et al. (2021)	Smartphone security	Cybersecurity policies, technological factors, and cultural differences predict intention toward smartphone security.	PMT; GDT; TRA	Smartphone-specific technology, Threat susceptibility; Threats vulnerability; Self-efficacy; Behavioral intention;	√				√	√	
Bélanger and Crossler (2019)	Mobile protective behavior	Mobile privacy protection self-efficacy predicts mobile information protection intentions	TPB,	Mobile trust, mobile privacy concerns, attitude toward information sharing, behavioral intentions	√				√		√
Crossler and Bélanger (2019)	Smartphone security	Individual privacy skills influence their motivational behavior toward mobile privacy-protective behavior	SET; IMBS	Privacy risk awareness; privacy knowledge; Privacy self-efficacy; technology self-efficacy, privacy behavior	√				√		√
Verkijika (2018)	Smartphone security	Anticipated regret and smartphone	PMT	Anticipated regret, perceived	√				√	√	

(continued on next page)

(*continued*)

Protection Literature			Protection Concepts		Current Research Emphasis		Protection Gaps	
							Gap1	Gap2
		security intentions positively influenced smartphone security behaviors		vulnerability, severity, self-efficacy, response efficacy, security intention, security behavior				
Crossler and Bélanger (2017)	Mobile privacy and security	Identifying the Mobile privacy-security knowledge gap	IMBS	Information awareness; Motivation, Security knowledge; Privacy knowledge; Self-efficacy; Security behavior	√		√	√
Thompson et al. (2017)	Mobile security behavior	Some of the determinants of security behavior differ between home computer and mobile device use	PMT	Perceived vulnerability, self-efficacy, response cost, descriptive norm, security intention, security behavior		√	√	√
Chen and Li (2017)	Mobile defensive behavior	Privacy concerns and coping appraisal have a significant impact on the intention to adopt the security defensive software	TTAT	Perceived concerns, Self-efficacy; Perceived cost; Privacy security awareness; Privacy security assurance behavior	√	√	√	√
Wang et al. (2016)	Mobile Privacy and information disclosure	Perceived mobile benefits and privacy risks explain the intention to disclose information via a mobile application	PCT	Perceived severity; Perceived risks; Perceived control; intention to disclose	√		√	√
Tu et al. (2015)	Mobile theft and information security risk	Coping appraisal and threat appraisal explain coping intention toward mobile threats	PMT; SLT	Self-efficacy; Response efficacy; perceived threat; experience; Knowledge; Social influence	√		√	√
Mylonas et al. (2013)	Understand the impact of trusting mobile third-party apps on mobile users' security	Smartphone users do not have the proper security awareness to make appropriate security decisions regarding authorizing 3rd party applications to access their mobile devices.	ISA	Users Awareness; Users' trust, IT Expertise; Privacy concerns;	√	√	√	√

Note: PMT: Protection motivation theory; GDT: General deterrence theory; TRA: Theory of reasoned actions; TPB: Theory of planned behavior; EDT: Expectation-disconfirmation theory; SET: Self-efficacy theory; IMBS: Information–motivation–behavioral skills model; TTAT: Technology threat avoidance theory; PCT: Privacy calculus theory. SLT: Social learning theory; ISA: Information Security Awareness.

Appendix 2. The conceptualization of EVT in information security literature

Author	Research				Expectancy and Motivational Values				
	Context	Objective	Environment		Conceptualization	Protection Gaps			
			PC	Mob		Expt	Cap	Tech	Mot
Hann et al. (2007)	Online Privacy	Examine how to overcome online information privacy concerns.	✓	x	Use protection values as positive valences that motivate users and expect their decision to mitigate privacy concerns	✓	x	x	✓
Wang et al. (2008)	ISec Investment	Understand the impact of security risk value on loss expectancy and ISec investment	✓	x	Introduce the value-risk concept to measure expected losses due to security exploits in organizations	✓	x	x	✓
Myyry et al (2009)	ISec Policies Adherence	Understand the impact of ISP values on ISec rules adherence	✓	x	Hypothesize values as motivations that predict ISP compliance	x	✓	x	✓
Bulgurcu et al. (2010)	ISec Policies Compliance	Understand the role of ISP awareness and benefits on ISP intentions	✓	x	Measure how employees value the benefits of ISP	x	✓	x	✓
Liu and Goodhue (2012)	E-commerce	The impact of trust on user's new visitor's intention to revisit a website	✓	x	Conceptualize EVT and cognitive misers' concepts on trust as a value that explains the intention to revisit	x	x	x	✓
Sun et al. (2012)	Knowledge sharing	Understand the sustained participation in knowledge sharing in transactional virtual communities.	✓	x	conceptualize extrinsic and intrinsic motivation constructs to predict continuance intentions.	x	✓	x	✓
Chen (2013)	self-disclosure	Examines voluntary self-disclosure phenomenon among social networking sites.	✓	x	Develop privacy value as a moderator on the relationship between attitude and privacy self-disclosure behavior.	x	x	x	✓
Tamjidyamcholo et al. (2014)	Knowledge sharing	Understand the impact of knowledge-sharing behavior on users' expectations to reduce ISec risk	✓	x	Conceptualize values as expected consequences of behavior and expectations to measure ISec risk reduction	✓	x	x	✓
D'Arcy and Lowry (2019)	ISec compliance	Examine the Cognitive-Affective Drivers of Employees' behavior toward ISec compliance behavior	✓	x	Conceptualize moral considerations as motivational values that explain compliance behavior	x	✓	x	✓
Turel et al. (2021)	ISec Policy Violation	Understand the persistence of ISP violations from the perspective of value/gain	✓	x	ISP violations are likely motivated by the expected value, benefits, or gains that an individual produces	✓	x	x	✓
Pereira and Mohiya (2021)	Knowledge Sharing	Investigate positive and negative employee's intentions of knowledge-sharing and hiding	✓	x	Use EVT to utilize the Expectancy and valence to theorize motivation for knowledge-sharing behavior	✓	x	x	✓
Wall et al. (2021)	ISec control portfolios	Understand how these security controls influence employees' behaviors	✓	x	Conceptualize the values as intrinsic and extrinsic motivations	x	✓	✓	✓
This Study	**Mobile Identity Protection**	**Examine the role of protection awareness and experience in bridging the gaps in mobile identity protection**	**x**	✓	**Use EVT to conceptualize and examine protection gaps in the mobile identity protection context**	✓	✓	✓	✓

Appendix 3. The interviewees' profiles

NO.	Stakeholders Group	Respondent Role	Years of experience	Role description
R1	Customer-facing bankers	Retail banker	11	Counseling customers on banking products and services
R2		Personal banker	13	Managing client bank accounts, including opening, and closing accounts, and supervising transactions.
R3		customer service adviser	10	Provide face-to-face bank services with the customers
R4		Senior Teller	18	Responsible for all aspects of front-end customer services
R5	IT	Business intelligent analyst	10	Analyze the bank's data and information to provide insights for decision-makers to improve performance and profitability
R6		IT service desk agent	12	Receive customer's technical requests and direct them to the correspondence IT department to resolve the related problems and IT incidents and may escalate the complaint based on the bank's escalation matrix.
R7		IT Security Specialist	11	Designing and implementing safety measures, policies, and security controls.
R8		IT service management (ITSM) analyst	10	Monitor, analyze, and assess the service desk tickets to understand the customers' requirements and improve the business process.
R9		Information security professional	16	Monitor the bank's networks for any security breaches or policy violations and install security software, such as firewalls, intrusion prevention, and data encryption programs, to protect the bank's sensitive information.
R10		Mobile application security analyst	10	Provide security assessment of the bank mobile application and help in designing the security strategy for the bank mobile infrastructure.
R11		Technical support agent	12	Answer customers' phone calls provide them the technical support and solve the reported problems.
R12		Help Desk Agent	10	Bridging between the customer's technical support requests and the IT department.
R13		e-Banking mobile application developer	10	Analyze, design, and develop an application for the bank mobile app such as electronic wallet and OTP apps.
R14	Manager	Chief Information Security Officer (CISO)	20	Develop the bank's information security strategy and implement the security programs, procedures, and policies to protect the bank's infrastructure and services against internal and external threats and related attacks.

(*continued on next page*)

(*continued*)

NO.	Stakeholders Group	Respondent Role	Years of experience	Role description
R15		IT Operation Manager	17	Monitoring and managing the network infrastructure and resolving system issues in the operating environment.
R16		Quality Manager	16	Ensure that all bank's products and services meet quality standards before they go live.
R17		Branch Manager	12	Manage bank's services including budget allocation, and sales plans, and coordinate with other branches as well as the main branch.
R18		RISK Manager	15	Manage and communicate the risk policies in the bank.
R19		Asset Manager	11	Manage the bank's software and hardware assets and coordinate with bank managers to assess the bank's actual needs and optimize the current bank's resources
R20		Audit Manager	14	Manage and Assess the deployed bank security policies and risk management activities.
R21		IT service manager	19	Manage the tasks and services of the information technology department and coordinate between business and IT.

Appendix 4. Interview guidelines

Category/Subcategory	Open-ended questions
Protection Experience	1. What experience have you had regarding mobile identity protection with yourself or with the bank's customers?
	2. How did you solve the problem?
Technical Means of Protection	3. What is your opinion on using multi-factor authentication to secure the individual's identity while using a mobile banking application?
	4. What is your opinion of using third-party security software for protecting mobile identity?
	5. What are your suggestions regarding effective ways to protect mobile users' identities?
	6. How would you improve mobile identity protection?
Protection Capabilities	7. Do you think that bank customers could protect their mobile identity while using Internet banking or mobile banking applications?
Protection Awareness	8. What would happen if your bank customers lost their mobile or their identity got stolen?
	9. What is the role of protection awareness in mobile identity protection?
Motivation-technical gap	10. What are the technical measures taken by the bank to protect customers' mobile identity?
	11. How does motivation influence the bank's customers to enable security measurement to protect their identities?
	12. Do you think that technical protection is enough to protect mobile users' identities and why?
	13. What are the reasons behind identity theft?
	14. Based on your experience, is the customer capable of protecting his/her identity without the bank's support?
Protection Motivation	15. What motivates customers to protect their mobile identities?
Protection Expectations	16. What makes customers expect they would secure their mobile identity?
Confidence	17. In your opinion, what are the factors that affect the customers' confidence regarding securing their mobile identity?
Importance	18. Why do you believe that mobile identity protection is important on the Internet and mobile banking environments?
Protection value	19. To what extent do customers value bank security measures to protect their identities against different fraud attacks?
Expectancy-Capability gap	20. Is there a difference between individuals' expectations and their capabilities in protecting their mobile identity?
	21. What is your perception of individuals' expectations to succeed in protecting the customer's mobile identity?
	22. What is your perception of the customers' actual capabilities in protecting their mobile identity?
	23. How do you think customers' expectations influence their mobile identity protective behavior compared to their actual protection capabilities?

Appendix 5. The emergent themes and quotes by the interview respondents

Higher-level category \subcategory	Emergent concepts/ themes/variables	Respondents																				
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
Protection Expectancy	Experience	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
	Vicarious Experience		x		x		x		x		x	x			x	x			x			
	Confidence	x	x		x	x			x		x	x	x		x		x	x	x			
	Importance	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		x	x	x		x
Expectancy-Capability gap	Protection expectancy	x	x	x		x	x	x		x		x	x		x	x	x	x		x	x	
	Protection Capability	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	
Protection value motivation	Extrinsic motivation	x			x	x		x	x		x			x	x	x	x	x	x			
	Intrinsic motivation					x			x		x			x	x	x			x			
	Achievement motivation				x	x		x	x		x	x		x	x	x		x	x			x
	Social motivation		x				x	x			x			x					x		x	
motivation-technical gap	Protection value	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		x	x
	Technical Protection	x	x	x	x	x	x	x		x		x	x	x	x	x	x	x	x	x		x
Protection behavior	Protection Awareness	x	x	x	x	x	x	x	x	x		x		x	x	x	x	x	x	x	x	x
	Mobile identity protection intention	x	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	x			x

Appendix 6. Hypotheses developed from the literature and in-depth interviews

Categories	Emergent concepts	Interviewee	Sample interview quotes	Supporting literature	Hypothesis
Protection Expectancy (PE) Protection Capability (PC)	Experience (Exp)	Mobile application security analyst	*"... our analysis indicates that seniors and customers with only a high school diploma are more vulnerable to mobile identity theft, account takeover, and stealing credit card numbers"*	The most effective way to build individual capability is through the mastery of experiences (Bandura, 2008).	H1a: Exp (-) → PC H1b: Exp (+) → PC H2a: Exp (-) mod (PM → MIPI) H2b: Exp (-) mod (PE → MIPI)
	Experience (Moderator)	Personal banker	*"..... what I have seen is that people who have been using our mobile applications for a while seem to have a better attitude and posture towards identity protection.... "*	Experience may moderate relationships among users' attitudes, intentions, and behavior (e.g., Churchill, 1979; Cron et al., 1988)	H2c: Exp (-) mod (TPA → MIPI) H2d: Exp (+) mod (PV → MIPI) H2e: Exp (+) mod (PA → MIPI)
	Vicarious Experience (VExp)	IT Service desk agent	*".... when I inquire about the reason for using the same old password again, they usually reply that they asked others to help them to understand how OTP works, and they follow their suggestions instinctively."*	The actual behavior of others concerning the technology is a further source of an individual's self-efficacy and outcome expectations (Compeau and Higgins, 1995).	H3a. VExp (+) → PC H3b: VExp (+) → PE
	Confidence (Conf)	Retail bankers	*"... I see first-hand how over time, customers have become confident in the use of mobile applications. Ever since COVID-19, we saw a dramatic increase ...."*	There are many activities that, if done well, guarantee valuable outcomes, but persons who doubt their ability to succeed (i.e., lack of confidence) will not likely pursue these behaviors (Betz and Hackett, 1981)	H4a. Conf (+) → PC H4b. Conf (+) → PE
	Importance (Imp)	IT service management (ITSM) analyst	*"... I found that most of these tickets involved a situation where a fraudster had used a customer's identity to make purchases. ..... However, stolen identity is a completely different issue. Dealing with such complaints is complex".*	Both the perceived task's importance and users' confidence influence their behavior toward achieving the required task (Feather 1982).	H5a. Imp (+) → PC H5b: Imp (+) → PE
Expectancy-Capability gap	**Protection expectancy**	QA Manager	*".... I found that many OTP passwords were formerly resolved and had been reopened. At our bank, we regularly conduct a root cause analysis. We found that user expectation for using electronic wallets is far beyond their actual capability. I attribute this to a lack of training."*	The individuals' actions are related to their subjective value of behavioral outcomes and the expectancy or probability of conducting the behavior successfully and achieving outcomes (Rasch and Tosi, 1992).	H11A: PE (+) → MIPI H11B: PE (+) → PA
	Protection Capability	IT Operation Manager	*"... Recently we found that our electronic wallet is the most frequently used application in online transactions. Interestingly, we also found that most support tickets involve difficulty in using multi-factor authentication and configuring Biometric authentication for mobile banking apps".*	The individual's beliefs about their capabilities are critical elements of the relationship between human behavior and motivation (Bandura, 1986)	H10A: PC (+) → MIPI H10B: PC (+) → PA
Protection value	Extrinsic motivation (EM) Intrinsic motivation (IM) Achievement motivation (AM) Social motivation (SM)	Chief information security officer (CISO)	*"...., it is really hard to prevent savvy criminals from stealing our customers' bank accounts using different identity fraud techniques. As a result, we decided to create a customer-centric security strategy that focuses on how to motivate our customers to apply identity protection measures. We are thinking of developing an award point system where enabling biometric multifactor authentication on our electronic wallet earns certain cashback points."*	Menard et al. (2017) argue that motivational aspects direct users' activity and influence them to comply with security measures and take action to protect information assets. Feather (1982) posits that achievement motivation, which allows ego enhancement, and social motivation, which is considered what people value, can be added to the categories of extrinsic and intrinsic motivation.	H6. EM (+) → PV H7: IM (+) → PV H8. AM (+) → PV H9: SM (+) → PV
Motivation-technical gap	**Protection value**	Information security professional	*"... Regardless of the different identity theft techniques used, the common factor between all these incidents is that our customers do not realize how valuable their digital identities are until they get scammed."*	Shah and Higgins (1997) suggested that as value increases, the effect of value on behavioral intentions increases as well. Whereas Menard et al. (2017) argue that motivation directs users' activity and influences them to comply with security policies and take action to protect information assets.	H13A: PV (+) → TPA H13B: PV (+) → MIPI
	Technical protective actions	Branch Manager	*"..... Many individuals trust Android and iOS platforms to protect their mobile identity. However, this trust will not make them bulletproof against identity theft attacks".*	Alnajim and Munro (2009) suggested that user-related technical abilities and phishing awareness are two critical factors that influence the protective actions of users against the usage of phishing websites.	H12: TPA (+) → MIPI
Protection Behavior	Protection Awareness (PA)	Technical support agent	*"... Usually, this type of support takes more than 5–7 minutes. However, during the conversation with the client, I discovered that she worked in IT and had a conceptual understanding of biometric authentication."*	Allam et al. (2014) argued that mobile users are not aware of the security risks associated with the use of smartphone applications due to their ineffective protective behavior.	H14: TPA (+) → MIPI

(*continued on next page*)

(*continued*)

Categories	Emergent concepts	Interviewee	Sample interview quotes	Supporting literature	Hypothesis
	Protection Awareness (**Mediator**)	Help Desk Agent	*One user justified his account loss: "I just don't think I have any important information that hackers would be interested to take from me. So, I thought that protecting my online identity was not that important."*	Haeussinger and Kranz (2013) suggested that information security awareness (ISA) is one of the most important antecedents of security behavior. He argued that by investigating the important, yet understudied, mediating role of ISA on the relation between awareness antecedents and the intention to achieve security actions.	Mediation effect of Awareness on the relations: PC&MIPI and PE&MIPI

Appendix 7. The measurement items

Construct	Items	Instrument	Refs.
Experience (Exp)	Expr1	Protecting my mobile identity is a new experience for me (Strongly Disagree – Strongly Agree)	Karahanna et al. (2006)
	Expr2	Protecting my mobile identity is not similar to anything that I've done before (Strongly Disagree – Strongly Agree)	
	Expr3	Protecting my mobile identity is different from other experiences I have had (Strongly Disagree – Strongly Agree)	
	Expr4	Protecting my mobile identity is a new business experience for me (Strongly Disagree – Strongly Agree)	
Vicarious Experience (VExp)	VExp1	Respondents were asked to indicate the extent to which mobiles with protected identity were actually used by:	
	VExp2	their peers in their work organization	
	VExp3	their peers in other organization	
	VExp4	their family	
	VExp5	their friends	
	VExp6	their managers	
	VExp7	other management	
Confidence (Conf)	Conf1	How good at mobile identity protection are you? (not at all good - very good)	Wigfield and Eccles (2000)
	Conf2	If you were to list all the mobile users in your friends from the worst to the best in mobile identity protection, where would you put yourself? (one of the worst - one of the best)	
	Conf3	Some mobile users are better at mobile tasks than others. For example, you might be better at gaming than in Identity Protection. Compared to most of your other mobile tasks, how good are you in Identity Protection? (a lot worse in Identity Protection than in other tasks - a lot better in Identity Protection than in other tasks)	
Importance (Imp)	Imp1	For me, being good in mobile identity protection is (not at all important - very important)	Wigfield (1994)
	Imp2	Compared to most of your other mobile activities, how important is it for you to be good at mobile identity protection? (not at all important - very important)	
	Imp3	Is the amount of effort it will take to protect your mobile identity worthwhile to you? (not very worthwhile, very worthwhile)	Eccles and Wigfield (1995)
	Imp4	I feel that, to me, being good in protecting my mobile identity which involves protective actions is (not at all important, very important)	
Protection Capability (PC)	PC1	Based on my own knowledge, skills, and capabilities, protecting my mobile identity would be easy for me	Kim and Kankanhalli (2009)
	SC2	I am capable to protect my mobile identity without the help of others (Strongly Disagree – Strongly Agree)	
	SC3	I am capable to protect my mobile identity reasonably well on my own (Strongly Disagree – Strongly Agree)	
Protection Expectancy (PE)	PE1	Compared to other mobile users, how well do you expect to do in protecting your mobile identity? (not at all well - very well)	Wigfield (1994)
	PE2	How well do you think you will do in using mobile identity protection features? (not at all well - very well)	
	PE3	How well do you expect to do in protecting your mobile identity? (not at all well - very well)	Wigfield and Eccles (2000)
	PE4	How good would you be at learning something new in mobile identity protection? (not at all good - very good)	
Achievement Motivation (AM)	AM1	How important is it for you to act like most of the mobile users regard protecting your mobile identity? (not at all important, very important)	Wigfield (1994)
	AM2	Do you think being good at mobile identity protection is more important for males than for females? (Strongly Disagree – Strongly Agree)	
Intrinsic Motivation (IM)	IM1	In General, I find protecting my mobile identity is (extremely boring – Extremely interesting)	Eccles and Wigfield (1995)
	IM2	How much do you like protecting your mobile identity? (Too little – Too much)	
	IM3	How much do you feel internally driven to protect your mobile identity? (Too little – Too much)	Designed for the study
Extrinsic Motivation (EM)	EM1	How useful is learning mobile identity protection for what you usually do with your other mobile activities? (not at all useful, very useful)	Eccles and Wigfield (1995)
	EM2	How useful is what you learn in mobile identity protection for your other daily life activities? (not at all useful, very useful)	
	EM3	How useful is external motivation in achieving mobile identity protection? (not at all useful, very useful)	Designed for the study
Social Motivation (SM)	SM1	People who are important to me think that I should protect my mobile identity (Strongly Disagree – Strongly Agree)	Venkatesh et al. (2012)
	SM2	People who influence my behavior think that I should protect my mobile identity (Strongly Disagree – Strongly Agree)	
	SM3	People whose opinions that I value prefer that I protect my mobile identity (Strongly Disagree – Strongly Agree)	

(*continued on next page*)

(*continued*)

Construct	Items	Instrument	Refs.
Motivation Value (MV)	MV1	I am keen to learn a lot about mobile identity protection (Strongly Disagree – Strongly Agree)	Trautwein et al. (2012)
	MV2	Mobile identity protection is important to me personally (Strongly Disagree – Strongly Agree)	
	MV3	It is important to me personally to be good at mobile identity protection (Strongly Disagree – Strongly Agree)	
Technical protective (TP)	When it comes to the effectiveness of technical protective actions against mobile identity threats, I believe that		Chen and Zahedi (2016)
	TP1	the success rate of mobile identity technical protective actions is (very low/very high)	
	TP2	the chance of stopping identity theft attacks by taking technical protective actions is (very low/very high)	
	TP3	the likelihood to neutralize mobile identity threats is (very low/very high)	
	TP4	my confidence in the effectiveness of mobile technical identity protective actions is (very low/very high)	
Protection awareness (PA)	PA1	Overall, I am aware of the mobile identity threats and their negative consequences (Strongly Disagree – Strongly Agree)	Bulgurcu et al. (2010)
	PA2	I have sufficient knowledge about the cost of potential identity theft problems (Strongly Disagree – Strongly Agree)	
	PA3	I understand the concerns regarding mobile identity protection and the risks they pose in general (Strongly Disagree – Strongly Agree)	
Mobile identity protection intention (MIPI)	MIPI1	I intend to protect my mobile identity (Strongly Disagree – Strongly Agree)	Taylor and Todd (1995)
	MIPI2	I intend to use my mobile using (Face, fingerprint, passwords, or PIN) identity protection features (Strongly Disagree – Strongly Agree)	
	MIPI3	I intend to protect my mobile identity frequently (Strongly Disagree – Strongly Agree)	

References

Ajzen, I., Fishbein, M., 1975. A Bayesian analysis of attribution processes. Psychol. Bull. 82 (2), 261.

Albrechtsen, E., 2007. A qualitative study of users' view on information security. Comput. Secur. 26 (4), 276–289.

Allam, S., Flowerday, S.v, Flowerday, E., 2014. Smartphone information security awareness: A victim of operational pressures. Comput. Secur. 42, 56–65.

Alnajim, A., Munro, M., 2009. An anti-phishing approach that uses training intervention for phishing websites detection. *2009 Sixth International Conference on Information Technology: New Generations*, pp. 405–410.

Ameen, N., Tarhini, A., Shah, M.H., Madichie, N., Paul, J., Choudrie, J., 2021. Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce. Comput. Hum. Behav. 114, 106531.

Bandura, A., 1986. Social foundations of thought and action. Englewood Cliffs, NJ, pp. 94–106.

Bandura, A., 1997. Self-efficacy: The exercise of control. Self-Efficacy: The Exercise of Control. W H Freeman/Times Books/Henry Holt & Co.

Bandura, A., 2008. An agentic perspective on positive psychology. Posit. Psychol. 1, 167–196.

Bandura, A., Freeman, W.H., Lightsey, R., 1999. Self-Efficacy: The Exercise of Control. Springer.

Bélanger, F., Crossler, R.E., 2019. Dealing with digital traces: Understanding protective behaviors on mobile devices. J. Strateg. Inf. Syst. 28, 34–49.

Betz, N.E., Hackett, G., 1981. The relationship of career-related self-efficacy expectations to perceived career options in college women and men. J. Couns. Psychol. 28 (5), 399–410.

Bose, I., Leung, A.C.M., 2019. Adoption of identity theft countermeasures and its short- and long-term impact on firm value. MIS Q. 43 (1).

Braver, T.S., Krug, M.K., Chiew, K.S., Kool, W., Westbrook, J.A., Clement, N.J., Adcock, R.A., Barch, D.M., Botvinick, M.M., Carver, C.S., 2014. Mechanisms of motivation–cognition interaction: challenges and opportunities. Cognitive, Affective, & Behavioral Neuroscience 14, 443–472.

Bubukayr, M.A.S., Almaiah, M.A., 2021. Cybersecurity concerns in smart-phones and applications: A survey. In: Proceedings of the International Conference on Information Technology (ICIT), pp. 725–731.

Bulgurcu, B., Cavusoglu, H., Benbasat, I., 2009. Effects of individual and organization based beliefs and the moderating role of work experience on insiders' good security behaviors, 2009 Int. Conf. Comput. Sci. Eng. 3, 476–481.

Bulgurcu, B., Cavusoglu, H., Benbasat, I., 2010. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Q. 34, 523–548. Management Information Systems(SPEC. ISSUE 3).

Burton, F.G., Chen, Y.N., Grover, V., Stewart, K.A., 1992. An application of expectancy theory for assessing user motivation to utilize an expert system. J. Manag. Inf. Syst. 8 (4), 183–198.

Califf, C.B., Sarker, S., Sarker, S., 2020. The bright and dark sides of technostress: A mixed-methods study involving healthcare IT. MIS Q. 44 (2).

Carter, M., Grover, V., 2015. Me, my self, and I (T) conceptualizing information technology identity and its implications. MIS Q. 39 (4), 931–958.

Carter, M., Petter, S., Grover, V., Thatcher, J.B., 2020. Information technology identity: A key determinant of IT feature and exploratory usage. MIS Q. 44 (3).

Caruccio, L., Desiato, D., Polese, G., Tortora, G., Zannone, N., 2022. A decision-support framework for data anonymization with application to machine learning processes. Inf. Sci. 613, 1–32.

Castillo-Montoya, M., 2016. Preparing for interview research: the interview protocol refinement framework. Qual. Rep. 21 (5).

Chen, R., 2013. Living a private life in public social networks: An exploration of member self-disclosure. Decis. Support Syst. 55 (3), 661–668.

Chen, H., Li, W., 2017. Mobile device users' privacy security assurance behavior: A technology threat avoidance perspective. Inf. Comput. Secur. 25 (3), 330–343.

Chen, Y., Zahedi, F.M., 2016. Individuals' internet security perceptions and behaviors: Polycontextual contrasts between the United States and China. MIS Q. 40 (1), 205–222.

Churchill Jr, G.A., 1979. A paradigm for developing better measures of marketing constructs. J. Mark. Res. 16 (1), 64–73.

Compeau, D.R., Higgins, C.A., 1995. Computer self-efficacy: Development of a measure and initial test. MIS Q. 19 (2), 189–211.

Craig, K., Thatcher, J.B., Grover, V., 2019. The IT identity threat: a conceptual definition and operational measure. J. Manag. Inf. Syst. 36 (1), 259–288.

Crespo, Á.H., Sánchez, Salmones, de los, M.M.G., Bosque, I.R.del, 2013. Influence of users' perceived compatibility and their prior experience on B2C e-commerce acceptance. Electronic Business and Marketing. Springer, Berlin, Heidelberg, pp. 103–123.

Crossler, R.E., Bélanger, F., 2017. The mobile privacy-security knowledge gap model: understanding behaviors. Proceedings of the 50th Hawaii International Conference on System Sciences, pp. 4071–4080.

Cron, W.L., Dubinsky, A.J., Michaels, R.E., 1988. The influence of career stages on components of salesperson motivation. J. Mark. 52 (1), 78–92.

Crossler, R.E., Bélanger, F., 2019. Why would I use location-protective settings on my smartphone? Motivating protective behaviors and the existence of the privacy knowledge–belief gap. Inf. Syst. Res. 30 (3), 995–1006.

D'Arcy, J., Lowry, P.B., 2019. Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. Inf. Syst. J. 29 (1), 43–69.

Donalds, C., Osei-Bryson, K.-M., 2020. Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. Int. J. Inf. Manag. 51, 102056.

Eccles, J., 1983. Expectancies, values, and academic behaviors. Achievement and achievement motives. Freeman and Company, San Francisco, pp. 75–138.

Eccles, J., Wigfield, A., 1995. In the mind of the actor the structure of adolescents achievement task values and expectancy related beleifs.pdf. Personality and Social Psychology Bulletin. Society for Personality and Social Psychology, Inc, pp. 215–255.

ENISA, (2020). Identity theft report: ENISA threat landscape. Retrieved from https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl-2020-identity-theft. Accessed 20 January 2023.

Ericson, 2023. Ericsson Mobility Report. Retrieved from https://www.ericsson.com/en/reports-and-papers/mobility-report. Accessed 22 April 2022.

Feather, N., 1982. Expectations and actions: Expectancy-value models in psychology. Lawrence Erlbaum Assoc Incorporated.

Feher, Katalin., 2019. Digital identity and the online self: Footprint strategies–An exploratory and comparative research study. J. Inf. Sci. 0165551519879702.

Fornell, C., Larcker, D.F., 1981. Structural equation models with unobservable variables and measurement error: Algebra and statistics. SAGE Publications Sage CA, Los Angeles, CA.

Fox, W., 2007. Managing organizational behavior. Juta and Company Ltd.

Gartner, (2022). Gartner unveils the top 10 government technology trends for 2022. Retrieved from https://www.gartner.com/en/newsroom/press-releases/2022-02-21-govt-tech-trends-2022-press-release.

Goodyear, P., Jones, C., Asensio, M., Hodgson, V., Steeples, C., 2004. Undergraduate students' experiences of networked learning in UK higher education: A survey-based study. Advances in research on networked learning, pp. 91–121.

Haeussinger, F., Kranz, J., 2013. Information Security Awareness: Its Antecedents and Mediating Effects on Security Compliant Behavior. In: Proceedings of the 15th International Conference on Information Systems (ICIS). Italy. San MilanPaper 1149.
Hair, J.F., Sarstedt, M., Ringle, C.M., Mena, J.A., 2012. An assessment of the use of partial least squares structural equation modeling in marketing research. J. Acad. Mark. Sci. 40 (3), 414–433.
Hann, I.H., Hui, K.L., Lee, S.Y.T., Png, I.P.L., 2007. Overcoming online information privacy concerns: An information-processing theory approach. J. Manag. Inf. Syst. 24 (2), 13–42.
Hedström, K., Kolkowska, E., Karlsson, F., Allen, J.P., 2011. Value conflicts for information security management. J. Strateg. Inf. Syst. 20 (4), 373–384.
Henseler, J., Ringle, C.M., Sinkovics, R.R., 2009. The use of partial least squares path modeling in international marketing. New challenges to international marketing. Emerald Group Publishing Limited.
Higgins, E.T., 1987. Self-discrepancy: a theory relating self and affect. Psychol. Rev. 94 (3), 319.
Howard, G.S., Mendelow, A.L., 1991. Discretionary use of computers: An empirically derived explanatory model. Decis. Sci. 22 (2), 241–265.
Jiang, J.J., Klein, G., Carr, C.L., 2002. Measuring information system service quality: SERVQUAL from the other side. MIS Q. 145–166.
Johnson, R.E., Rosen, C.C., Djurdjevic, E., 2011. Assessing the impact of common method variance on higher-order multidimensional constructs. J. Appl. Psychol. 96 (4), 744.
Karahanna, E., Agarwal, R., Angst, C.M., 2006. Reconceptualizing compatibility beliefs in technology acceptance research. MIS Q. 30 (4), 781–804.
Kim, H.-W., Kankanhalli, A., 2009. Investigating user resistance to information systems implementation: A status quo bias perspective. MIS Q. 567–582.
Kirova, D., Baumöl, U., 2018. Factors that affect the success of security education, training, and awareness programs: a literature review. J. Inf. Technol. Theory Appl. 19 (4), 56–82.
Kominis, G., Emmanuel, C.R., 2007. The expectancy–valence theory revisited: Developing an extended model of managerial motivation. Manag. Account. Res. 18 (1), 49–75.
Kraus, L., Wechsung, I., Möller, S., 2017. Psychological needs as motivators for security and privacy actions on smartphones. J. Inf. Secur. Appl. 34, 34–45.
Kaspersky, 2020. IT threat evolution Q2 2020 Mobile statistics. Retreived from https://securelist.com/it-threat-evolution-q2-2020-mobile-statistics/98337/ Accessed 22 January 2022.
Landry, C.C., 2003. Self-efficacy, motivation, and outcome expectation correlates of college students' intention certainty. LSU Doctoral Dissertations, 1254. https://repository.lsu.edu/gradschool_dissertations/1254.
Leavitt, N., 2011. Mobile security: finally a serious problem? Computer 44 (6), 11–14.
Lee, G., Xia, W., 2010. Toward agile: an integrated analysis of quantitative and qualitative field data on software development agility. MIS Q. 34 (1), 87–114.
Lin, K.-M., 2011. e-Learning continuance intention: Moderating effects of user e-learning experience. Comput. Educ. 56 (2), 515–526.
Lindell, M.K., Whitney, D.J., 2001. Accounting for common method variance in cross-sectional research designs. J. Appl. Psychol. 86 (1), 114.
Liu, B.Q., Goodhue, D.L., 2012. Two worlds of trust for potential e-commerce users: Humans as cognitive misers. Inf. Syst. Res. 23 (4), 1246–1262.
MacKenzie, S.B., Podsakoff, P.M., Podsakoff, N.P., 2011. Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques. MIS Q. 35 (2), 293–334.
MacKinnon, D.P., 2008. Multivariate applications series. *Introduction to statistical mediation analysis*. Chicago, 1st ed. Routledge.
Melone, N.P., 1990. A theoretical assessment of the user-satisfaction construct in information systems research. Manag. Sci. 36 (1), 76–91.
Menard, P., Bott, G.J., Crossler, R.E., 2017. User motivations in protecting information security: Protection motivation theory versus self-determination theory. J. Man. Inf. Sys. 34 (4), 1203–1230.
Miles, M.B., Huberman, A.M., 1994. Qualitative Data Analysis: An Expanded Sourcebook. Sage.
Mylonas, A., Kastania, A., Gritzalis, D., 2013. Delegate the smartphone user? Security awareness in smartphone platforms. Comput. Secur. 34, 47–66.
Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., Vance, A., 2009. What levels of moral reasoning and values explain adherence to information security rules? An empirical study. Eur. J. Inf. Syst. 18 (2), 126–139.
Nolan, R.L., Wetherbe, J.C., 1980. Toward a comprehensive framework for MIS research. MIS Q. 1–19.
Ogbanufe, O., Pavur, R., 2022. Going through the emotions of regret and fear: revisiting protection motivation for identity theft protection. Int. J. Inf. Manag. 62, 102432.
Peer, E., Brandimarte, L., Samat, S., Acquisti, A., 2017. Beyond the Turk: alternative platforms for crowdsourcing behavioral research. J. Exp. Soc. Psychol. 70, 153–163.
Pereira, V., Mohiya, M., 2021. Share or hide? Investigating positive and negative employee intentions and organizational support in the context of knowledge sharing and hiding. J. Bus. Res. 129, 368–381.
Podsakoff, P.M., MacKenzie, S.B., Lee, J.-Y., Podsakoff, N.P., 2003. Common method biases in behavioral research: a critical review of the literature and recommended remedies. J. Appl. Psychol. 88 (5), 879.
Posey, C., Roberts, T.L., Lowry, P.B., Bennett, R.J., Courtney, J.F., 2013. Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. MIS Q. 1189–1210.
Rasch, R.H., Tosi, H.L., 1992. Factors affecting software developers' performance: an integrated approach. MIS Q. 16 (3), 395–413.
Rodriguez-Priego, N., Porcu, L., Kitchen, P.J., 2022. Sharing but caring: Location based mobile applications (LBMA) and privacy protection motivation. J. Bus. Res. 140, 546–555.
Roussos, G., Peterson, D., Patel, U., 2003. Mobile identity management: an enacted view. Int. J. Electron. Commer. 8 (1), 81–100.
Safa, N.S., von Solms, R., Furnell, S., 2016. Information security policy compliance model in organizations. Comput. Secur. 56, 70–82.
Saldaña, J., 2021. The coding manual for qualitative researchers. SAGE Publications Limited.
Sarker, S., Sahay, S., Lau, F., 2002. Teaching information systems development using "virtual team" projects. J. Inf. Educ. Res. 4 (1), 35–46.
Sclater, M., Bolander, K., 2004. Factors influencing students' orientation to collaboration in networked learning. Advances in research on networked learning. Springer, pp. 175–203.
Serrano, C., Karahanna, E., 2016. The Compensatory Interaction Between User Capabilities and Technology Capabilities in Influencing Task Performance. MIS Q. 40 (3), 597–622.
Shah, J., Higgins, E.T., 1997. Expectancy× value effects: Regulatory focus as determinant of magnitude and direction. J. Pers. Soc. Psychol. 73 (3), 447.
Sheffler, Z.J., Liu, D., Curley, S.P., 2020. Ingredients for successful badges: evidence from a field experiment in bike commuting. Eur. J. Inf. Syst. 1–16.
Snead, K.C., Harrell, A.M., 1994. An application of expectancy theory to explain a manager's intention to use a decision support system. Decis. Sci. 25 (4), 499–510.
Shen, A.X.L., Cheung, C.M.K., Lee, M.K.O., Chen, H., 2011. How social influence affects we-intention to use instant messaging: the moderating effect of usage experience. Inf. Syst. Front. 13 (2), 157–169.
Straub, D.W., 1989. Validating instruments in MIS research. MIS Q. 147–169.
Sun, Y., Fang, Y., Lim, K.H., 2012. Understanding sustained participation in transactional virtual communities. Decis. Support Syst. 53 (1), 12–22.
Tamjidyamcholo, A., Baba, M.S.B., Shuib, N.L.M., Rohani, V.A., 2014. Evaluation model for knowledge sharing in information security professional virtual community. Computers & Security, 43, pp. 19–34.
Taylor, S., Todd, P., 1995. Understanding information technology usage: a test of competing models. Inf. Syst. Res. 6 (2), 144–176.
Thompson, N., McGill, T.J., Wang, X., 2017. Security begins at home: Determinants of home computer and mobile device security behavior. Computers and Security, 70, pp. 376–391.
Trauth, E.M., Farwell, D.W., Lee, D., 1993. The IS expectation gap: Industry expectations versus academic preparation. MIS Q. 293–307.
Trautwein, U., Marsh, H.W., Nagengast, B., Lüdtke, O., Nagy, G., Jonkmann, K., 2012. Probing for the multiplicative term in modern expectancy–value theory: a latent interaction modeling study. J. Educ. Psychol. 104 (3), 763–777.
Tu, Z., Turel, O., Yuan, Y., Archer, N., 2015. Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination. Information & Management, 52, pp. 506–517.
Turel, O., He, Q., Wen, Y., 2021. Examining the neural basis of information security policy violations: a noninvasive brain stimulation approach. MIS Q. 45 (4), 1715–1744.
Van Maele, D., Van Houtte, M., 2012. The role of teacher and faculty trust in forming teachers' job satisfaction: Do years of experience make a difference? Teach. Teach. Educ. 28 (6), 879–889.
Venkatesh, V., Brown, S.A., Bala, H., 2013. Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. MIS Q. 21–54.
Venkatesh, V., Brown, S.A., Sullivan, Y.W., 2016. Guidelines for conducting mixed-methods research: An extension and illustration. J. Assoc. Inf. Syst. 17 (7), 2.
Venkatesh, V., Thong, J.Y.L., Xu, X., 2012. Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. MIS Q. 157–178.
Vedadi, A., Warkentin, M., 2020. Can secure behaviors be contagious? A two-stage investigation of the influence of herd behavior on security decisions. J. Assoc. Inf. Syst. 21 (2), 3.
Verkijika, S.F., 2018. Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret. Computers & Security, 77, pp. 860–870.
Virvilis, N., Tsalis, N., Mylonas, A., Gritzalis, D., 2014. Mobile devices: A phisher's paradise. In: Proceedings of the 11th International Conference on Security and Cryptography (SECRYPT), pp. 1–9.
Vroom, V.H., 1964. Work and motivation. Wiley & Sons, New York, NY.
Wall, J.D., Palvia, P., D'Arcy, J., 2021. Theorizing the behavioral effects of control complementarity in security control portfolios. Inf. Syst. Front. 1–22.
Walsham, G., 1993. Interpreting information systems in organizations. Wiley Chichester (Vol. 19).
Wang, J., Chaudhury, A., Rao, H.R., 2008. Research note—A value-at-risk approach to information security investment. Inf. Syst. Res. 19 (1), 106–120.
Wang, T., Duong, T.D., Chen, C.C., 2016. Intention to disclose personal information via mobile applications: A privacy calculus perspective. Int. J. Inf. Manage. 36 (4), 531–542.
Wigfield, A., 1994. Expectancy-Value Theory of Achievement Motivation: A Developmental Perspective. Educational Psychology Review 6, 49–78.
Wigfield, A., Eccles, J.S, 2000. Expectancy–value theory of achievement motivation. Contemp. Educ. Psychol. 25 (1), 68–81.
Wu, D., Moody, G.D., Zhang, J., Lowry, P.B., 2020. Effects of the design of mobile security notifications and mobile app usability on users' security perceptions and continued use intention. Inf. Manag. 57 (5), 103235.
Wunderlich, P., Veit, D.J., Sarker, S., 2019. Adoption of sustainable technologies: a mixed-methods study of German households. MIS Q. 43 (2), 673–691.
Zhang, R., Chen, J.Q., Lee, C.J., 2013. Mobile commerce and consumer privacy concerns. J. Comput. Inf. Syst. 53 (4), 31–38.